



Norton
Internet Security[™]
2004.
Professional

User's Guide

Norton Internet Security™ Professional User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 7.0

PN: 10103144

Copyright Notice

Copyright © 2003 Symantec Corporation. All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Standard Template Library

This product utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators.

Copyright © 1996-1999. Silicon Graphics Computer Systems, Inc.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright © 1994. Hewlett-Packard Company

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Trademarks

Symantec, the Symantec logo, Norton Internet Security, Norton Personal Firewall, LiveUpdate, Norton AntiSpam, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. Rescue Disk is a trademark of Symantec Corporation.

Microsoft, MS-DOS, MSN, Windows and the Windows logo are registered trademarks of Microsoft Corporation. AOL and CompuServe are registered trademarks of America Online, Inc. Pentium is a registered trademark of Intel Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Symantec License and Warranty

Norton Internet Security™ Professional

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "ACCEPT" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT ACCEPT" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE AND CONTACT SYMANTEC CUSTOMER SERVICE FOR INFORMATION ON HOW TO OBTAIN A REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE (LESS SHIPPING, HANDLING, AND ANY APPLICABLE TAXES) AT ANY TIME DURING THE SIXTY (60) DAY PERIOD FOLLOWING THE DATE OF PURCHASE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the property of Symantec, or its licensors, and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to You. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows.

You may:

- A. use one copy of the Software on each of two (2) single computers. If a License Module accompanies, precedes, or follows this license, You may make the number of copies of the Software licensed to You by Symantec as provided in Your License Module. Your License Module shall constitute proof of Your right to make such copies;
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

- C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
- D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and
- E. use the Software in accordance with any additional permitted uses set forth, below.

You may not:

- A. copy the printed documentation that accompanies the Software;
- B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
- D. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
- E. use a later version of the Software than is provided herewith unless You have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;
- F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;
- G. use the Software in any manner not authorized by this license; nor
- H. use the Software in any manner that contradicts any additional restrictions set forth, below.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as

requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit Licensee to obtain and use Content Updates.

3. Product Installation and Required Activation:

This Software may contain enforcement technology that limits the ability to install and uninstall the Software on a machine more than a finite number of times for a finite number of machines. This License and the Software containing enforcement technology require activation as further set forth in the Documentation. The Software will only operate for a finite period of time prior to Software activation by You. During activation, You will provide Your unique activation key accompanying the Software and PC configuration in the form of an alphanumeric code over the Internet to verify the authenticity of the Software. If You do not complete the activation within the finite period of time set forth in the Documentation, or as prompted by the Software, the Software will cease to function until activation is complete, which will restore Software functionality. In the event You are not able to activate the Software, You may contact Symantec Customer Support at the URL and telephone number set forth in the Documentation.

4. Sixty (60) Day Money Back Guarantee:

If You are the original licensee of this copy of the Software and are not completely satisfied with it for any reason, please contact Symantec Customer Service for a refund of the money You paid for the Software (less shipping, handling, and any applicable taxes) at any time during the sixty (60) day period following the date of purchase.

5. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR

IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

6. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

7. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

8. Export Regulation:

The Software and its related documentation, including technical data, may not be exported or re-exported in violation of the U.S. Export

Administration Act, its implementing laws and regulations, the laws and regulations of other U.S. agencies, or the export and import laws of the jurisdiction in which the Software was obtained. Export to any individual, entity, or country specifically designated by applicable law is strictly prohibited.

9. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales.

This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

This Software utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators. Copyright © 1996-1999. Silicon Graphics Computer Systems, Inc. Copyright © 1994. Hewlett-Packard Company.

Contents

Chapter 1	Responding to emergencies	
	If your product won't install	18
	If your computer won't start	19
	Scan for viruses using the CD	19
	Create Emergency Disks	20
	If you need to use Emergency Disks	21
	How to maintain protection	22
	Avoid viruses and threats	22
	Prepare for emergencies	23
 Chapter 2	 Feature summary	
	Activation protects you	26
	When to activate your product	26
	Locate the product key	26
	Security protection features	27
	Norton AntiSpam features	29
	Virus and threat protection features	31
	Advanced Utilities features	33
	Web Tools features	34
 Chapter 3	 Installing Norton Internet Security Professional	
	System requirements	35
	Supported email and instant messenger programs	37
	Compatibility with other software and hardware	37
	Before installation	39
	Prepare your computer	40

Install Norton Internet Security Professional	41
Customize your installation	45
If the opening screen does not appear	46
After installation	47
Use the Information Wizard	47
If you need to uninstall Norton Internet Security Professional	50

Chapter 4

Basics

Check the version number	53
Start Norton Internet Security Professional	54
Use the Norton Internet Security Professional tray icon	55
Use Web assistant from the Internet Explorer toolbar	56
Use your email program toolbar	57
Start Norton AntiVirus	58
Use the Norton AntiVirus icon in the Windows system tray	58
Use the Windows Explorer toolbar	58
Activate your product	60
Respond to Norton Internet Security Professional alerts	61
Learn more with the Alert Assistant	61
Use Web assistant	62
Check your computer's vulnerability to attack	62
Identify the source of Internet traffic	63
Stop all Internet communication	64
Manage how Norton AntiSpam detects spam	66
Adjust the email filter	66
Identify authorized senders	67
Identify senders of spam email messages	68
Teach Norton AntiSpam your email preferences	69
Manage advertising filters	71
Enable or disable Ad Blocking	71
Enable or disable Popup Window Blocking	72
Check Norton AntiVirus configuration status	73
Check Office Plug-in status	73

Transfer security settings to other computers	75
Configure settings	75
Export the settings file	76
Import the settings file	78
Temporarily disable Norton Internet Security	
Professional	79
Create and use Rescue Disks	80
About Rescue Disks	80
Create a Rescue Disk set	80
Test your Rescue Disks	82
Update your Rescue Disks	83
Rescue Disk options	83
If you need to use Rescue Disks to restore your	
system	84
For more information	86
Look up glossary terms	86
Use online Help	86
Readme file	87
Access the User's Guide PDF	88
Symantec products on the Web	88
Subscribe to the Symantec Security	
Response newsletter	90

Chapter 5

Options

Set Norton Internet Security Professional	
options	92
About General options	93
About LiveUpdate options	93
About Firewall options	94
About Email options	94
Password protect Norton Internet Security	
Professional options	94
Reset options password	94
Customize Norton AntiVirus	96
About System options	96
About Internet options	97
About Other options	98
Set Norton AntiVirus options	100
If you need to restore default Norton	
AntiVirus settings	100

Password protect Norton AntiVirus options	101
Set Wipe Info options	102

Chapter 6

Keeping current with LiveUpdate

About program updates	103
About protection updates	104
Obtain updates using LiveUpdate	105
When you should update	105
If you can't use LiveUpdate	105
Set LiveUpdate to Interactive or Express mode	106
Turn off Express mode	107
If you run LiveUpdate on an internal network	107
Run LiveUpdate automatically	108
About your subscription	110

Chapter 7

Guarding against intrusion attempts

About the Personal Firewall	111
Customize firewall protection	112
Change the Security Level	112
Change individual security settings	112
Allow or block access to your computer	114
Customize firewall rules	115
How firewall rules are processed	115
Create new firewall rules	116
Manually add a firewall rule	119
Change an existing firewall rule	120
Identify computers to Norton Internet Security	
Professional	121
Specify an individual computer	121
Specify a range of computers	122
Specify computers using a network	
address	122
About Intrusion Detection	123

Customize Intrusion Detection	124
Turn Intrusion Detection alerts on and off	124
Exclude specific network activity from being monitored	125
Enable or disable AutoBlock	126
Unblock AutoBlocked computers	127
Exclude computers from AutoBlock	127
Restrict a blocked computer	128

Chapter 8 Customizing protection for different locations

About Network Detector	129
Create a new location	130
Add new networks to locations	132
Learn more about networks	132
Customize a location's settings	133
Remove networks from a location	133
Delete a location	134

Chapter 9 Protecting disks, files, and data from viruses

Ensure that protection settings are enabled	135
Manually scan disks, folders, and files	136
Perform a full system scan	137
Scan individual elements	138
If problems are found during a scan	138
Create and use custom scans	139
Run a custom scan	140
Delete a custom scan	140
Schedule scans	141
Schedule a custom scan	141
Edit scheduled scans	142
Delete a scan schedule	143

Chapter 10 What to do if a virus is found

If a virus is found during a scan	146
Review the repair details	146
Use the Repair Wizard	146

If a virus is found by Auto-Protect	148
If you are using Windows 98/98SE/Me	148
If you are using Windows 2000/XP	149
If a threat is found by Worm Blocking	150
If Inoculation alerts you about a change in system files	151
If Norton AntiVirus places files in Quarantine	152
If Norton AntiVirus cannot repair a file	153
Look up viruses on the Symantec Web site	154

Chapter 11

Creating accounts for multiple users

About Norton Internet Security Professional accounts	156
Norton Internet Security Professional accounts and Windows accounts	156
Manage accounts on multiple computers	157
Create Norton Internet Security Professional accounts	157
Set the startup account	161
Set or change account passwords	161
Assign Norton Internet Security Professional account types to Windows accounts	162
Log on to Norton Internet Security Professional	163
Customize Norton Internet Security Professional accounts	164

Chapter 12

Controlling individuals' Internet use

About Productivity Control	165
Enable or disable Productivity Control	166
Customize Productivity Control	167
Restrict Web site access	167
Restrict programs that access the Internet	171
Restrict newsgroup access	172

Chapter 13

Protecting your privacy

Identify private information to protect	175
Add private information	176
Modify or remove private information	176

	Customize Privacy Control	177
	Set the Privacy Level	178
	Adjust individual Privacy Control settings	178
Chapter 14	Blocking unwanted email messages	
	Customize Norton AntiSpam	181
	Change the priority of a spam rule	183
Chapter 15	Blocking Internet advertisements	
	Use the Ad Trashcan	185
	Use text strings to identify ads to block	
	or permit	186
	How to identify Ad Blocking strings	186
	Add an Ad Blocking string	187
	Modify or remove an Ad Blocking string	187
Chapter 16	Recovering missing or erased files	
	About Norton Protection	189
	About UnErase Wizard	190
	Recover a file with UnErase Wizard	191
Chapter 17	Eliminating data permanently	
	About Wipe Info	193
	About hexadecimal values	194
	About the Government Wipe process	194
	Set Wipe Info options	195
	Wipe files or folders	196
Chapter 18	Improving Web browsing and connectivity	
	About Web Cleanup	199
	Delete unnecessary Web files	200
	View Web Cleanup files	200
	Exclude domains from Web Cleanup activity	203
	About Connection Keep Alive	205
	Enable or disable Connection Keep Alive	205
	View Connection Keep Alive status	206
	Set Connection Keep Alive options	206

Chapter 19	Monitoring Norton Internet Security Professional	
	View the Statistics window	210
	Reset information in the Statistics window	210
	Review detailed statistics	211
	View Norton Internet Security	
	Professional logs	212
	Review log information	212
	Monitor Norton AntiVirus activities	214
	About the Log Viewer	214
	Check the Activity Log	214
Chapter 20	Troubleshooting	
	Explore the Symantec service and support Web site	217
	Troubleshoot Norton Internet Security	
	Professional	219
	What is wrong with this Web site?	219
	Why can't I post information online?	220
	Why did an email message I sent never arrive?	220
	Why doesn't Norton Internet Security Professional notify me before letting programs access the Internet?	220
	Why can't I print to a shared printer or connect to a computer on my local network?	220
	How can a Web site get my browser information?	221

Troubleshoot Norton AntiSpam	222
Why do I still receive spam?	222
How will email messages from addresses on my Blocked list be handled?	222
What if I mistakenly put an address on the Blocked list?	222
Why did an email message someone sent me never arrive?	222
How do I keep my protection updated?	223
Why do I need a subscription to spam definitions?	223
Why does so much spam include clusters of meaningless characters?	223
Troubleshoot Ad Blocking	224
Does Ad Blocking block all advertising on the current page?	224
Will Popup Window Blocking block all pop-ups or only pop-up ads?	224
Are there security issues associated with advertisements?	224
Troubleshoot Norton AntiVirus	225
Auto-Protect does not load when I start my computer	225
I have scanned and removed a virus, but it keeps infecting my files	226
Norton AntiVirus cannot repair my infected files	227
I can't receive email messages	227
I can't send email messages	228
Troubleshoot Rescue Disks	229
My Rescue Disk does not work	229
I cannot start from drive A	230
I get an error when testing basic Rescue Disks	230

Service and support solutions

Glossary

Index

Responding to emergencies

1

If you have an emergency, read these sections to try to find the solution to your problem.

Common problems include:

- Virus *threats*
- Trouble restarting your computer
- Lost or missing files
- Possible disk damage



If you purchased this product to address any of the problems listed above, read these sections first. Immediate installation of the product may not always provide the best solution to your problem.

If your product won't install



You must be running Windows in order to install your Symantec product.

If you try to install and your computer has a virus and you choose not to run the Symantec Pre-Install Scanner, start over and run the Symantec Pre-Install Scanner as directed.

If you can't run the Symantec Pre-Install Scanner, but you can connect to the Internet, go to <http://security.symantec.com> and run virus detection from the Symantec Security Check Web site.

If you can't start your computer, you need to start from an uninfected disk and scan for viruses.

Once the virus has been repaired, delete the installation files that were left behind in the temporary folder after you tried to install the first time.


To delete remaining installation files

- 1 On the Windows taskbar, click **Start > Run**.
- 2 In the Run dialog box, type **%TEMP%**
- 3 Click **OK**.
- 4 In the Temp window, select all of the files that can be deleted. If system files are open, you will not be able to delete them. Just delete the ones that you can.
- 5 Click **Delete**.
- 6 Close the window.
- 7 After you delete the temporary files, begin installation again and run the Symantec Pre-Install Scanner to be sure that you have removed all of the viruses.

See "If your computer won't start" on page 19.

If your computer won't start

If you have a virus or threat on your computer, you need to start the computer from an uninfected disk to remove the virus.

Suggestion	For more information
Restart from the CD and scan your computer's hard disk for viruses.	See "Scan for viruses using the CD" on page 19.
Start your computer by using your Rescue Disks if you created them.  Rescue Disks are available only for Windows 98/Me.	See "Create and use Rescue Disks" on page 80.

Scan for viruses using the CD



You might need to change your computer's BIOS Setup options to start from the CD-ROM drive. To do so, see the documentation that came with your computer.

To start from the CD and scan for viruses

- 1 Insert the CD into the CD-ROM drive.
- 2 Restart your computer.
Your computer displays the following information:
 - 1 Boot from Hard Drive
 - 2 Boot from CD-ROM
- 3 Press **2 Boot from CD-ROM** to restart from the CD. After the computer restarts, the Emergency program automatically begins to scan for and remove viruses.
- 4 When Norton AntiVirus has finished scanning, remove the CD from your CD-ROM drive.

Create Emergency Disks

Emergency Disks are used to start your computer in case of a problem. If your computer can start from a CD, you can use the product CD in place of Emergency Disks and do not need to create them.

If you downloaded the software or do not have a CD, the program for creating Emergency Disks (NED.exe) is included in the download. Navigate to the location to which you downloaded the software and begin with step 3 of these instructions.

See "If you need to use Emergency Disks" on page 21.

If you cannot start your computer from a CD, you can use these instructions to create Emergency Disks on another computer or go to <http://www.symantec.com/techsupp/ebd.html> and download the Emergency Disk program. Follow the instructions included in the download to create the Emergency Disks.



You will need several formatted 1.44-MB disks.

To create Emergency Disks from the CD

- 1 Insert the CD into the CD-ROM drive.
- 2 Click **Browse CD**.
- 3 Double-click the **Support** folder.
- 4 Double-click the **Edisk** folder.
- 5 Double-click **NED.exe**.
- 6 In the welcome window, click **OK**.
- 7 Label the first disk as instructed and insert it into drive A.
- 8 Click **Yes**.
- 9 Repeat steps 7 and 8 for the subsequent disks.
- 10 When the procedure is complete, click **OK**.
- 11 Remove the final disk from drive A.
- 12 Test the first disk in the set to ensure that you can restart your computer with it.
- 13 Store the Emergency Disk set in a safe place.

If you need to use Emergency Disks

See ["Create Emergency Disks"](#) on page 20.

If you have not created Rescue Disks, you can use Emergency Disks to restart your computer and scan for viruses or run DOS-based recovery utilities.

To use Emergency Disks

- 1 Insert Emergency Disk 1 into drive A and restart your computer.
The Emergency program runs in DOS.
- 2 Select the program that you want to run.
For DOS program help, press the **F1** key while you are running the program.
- 3 Follow the on-screen instructions for inserting and removing the Emergency Disks.
- 4 When the Emergency program is done, remove the Emergency Disk from drive A and restart your computer.

How to maintain protection

When Norton AntiVirus is installed, you have complete virus protection. However, new viruses are created constantly. Viruses can spread when you start your computer from an infected disk or when you run an infected program. There are several things that you can do to avoid viruses and to recover quickly should a virus strike.

Avoid viruses and threats

It is important that you practice regular file maintenance and that you keep Norton AntiVirus up-to-date.

To avoid viruses:

- Write-protect removable media.
- Stay informed about viruses by logging on to the Symantec Security Response Web site (<http://securityresponse.symantec.com>) where there is extensive, frequently updated information on viruses and automatic virus protection.
- Keep LiveUpdate turned on at all times to continually update your virus definitions files.
- Run LiveUpdate regularly to receive new program updates.
- Keep Auto-Protect turned on at all times to prevent viruses from infecting your computer.
- If Auto-Protect is not turned on, scan removable media before you use them.
- Schedule periodic scans to occur automatically.
- Watch for email messages from unknown senders. Do not open anonymous attachments.
- Keep email protection turned on to avoid sending or receiving infected email attachments.
- Keep all recommended maximum protection settings turned on.

See "Explore the Symantec service and support Web site" on page 217.

See "Keeping current with LiveUpdate" on page 103.

See "Manually scan disks, folders, and files" on page 136.

See "Schedule scans" on page 141.

See "Ensure that protection settings are enabled" on page 135.

Prepare for emergencies

It is also important that you are prepared in case your computer is infected by a virus.

To prepare for emergencies:

- Back up files regularly and keep more than just the most recent backup.
- If you are using a computer that cannot start from a CD, create a set of Emergency Disks, from which you can start your computer and scan for viruses.
- If you are using Windows 98/Me, create a set of Rescue Disks and keep them updated. You can use them to start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems and recover from a system crash.

See ["Create and use Rescue Disks"](#) on page 80.



Feature summary

2

Use the information in this section to familiarize yourself with the product.

This section includes:

- A list of all of the features in the product
- A brief description of each feature

The feature summary can help you determine which feature to use to solve a problem. Read the feature descriptions to locate the correct component to use.

Activation protects you

Product activation is a technology that protects users from pirated or counterfeit software by limiting use of a product to those users who have acquired the product legitimately. Product activation requires a unique product key for each installation of a product. You must activate the product within 15 days of installing it.

Product activation is completely separate from registration. Your activation information and registration information reside on separate servers, with no link between the different sets of data.

When to activate your product

During installation, you are asked to enter a product key. After you have installed the product, activate it by sending the product key to the Symantec servers.

You can activate your product by clicking **Activate Now** in the Configuration Wizard that runs immediately after installation. If you choose not to activate at that time, you will receive [alerts](#) that will remind you to activate the product. You can click **Activate Now** in the alerts to activate the product. Activation should take just a few minutes.



If you do not activate the product within 15 days of installing it, the product will stop working. You can activate it after the 15 days have elapsed, but you will not be protected until you do.

Locate the product key

The product key can most frequently be found on a sticker on your CD sleeve. If it is not there, then it will be on an insert in your product package. If you have purchased the product on DVD, look for the sticker on your DVD package. If you have [downloaded](#) the product from the Symantec Store, the product key is stored on your computer as part of the download process.

Security protection features

Norton Internet Security Professional includes a suite of security tools that help keep your computer safe from viruses, security threats, unwanted email, and privacy intrusions.

Security protection features include:

Personal Firewall	<p>The Personal Firewall protects your computer from Internet attacks, dangerous Web content, port scans, and other suspicious behavior.</p> <p>See "About the Personal Firewall" on page 111.</p>
Intrusion Detection	<p>Intrusion Detection scans each piece of information that enters and exits your computer and automatically blocks any Internet attacks.</p> <p>See "About Intrusion Detection" on page 123.</p>
Network Detector	<p>Network Detector lets you customize security settings for different networks. This makes it easy for mobile users who connect to the Internet from the road to stay protected at all times.</p> <p>See "Customizing protection for different locations" on page 129.</p>
Web assistant	<p>Web assistant lets you customize security settings for individual Web sites without leaving your browser.</p> <p>See "Use Web assistant" on page 62.</p>
Privacy Control	<p>Privacy Control gives you several levels of control over the kind of information that users can send via the Web, email, and instant messenger programs.</p> <p>See "Protecting your privacy" on page 175.</p>
Ad Blocking	<p>Ad Blocking speeds up your Web surfing by eliminating banner ads, Flash presentations, pop-up and pop-under ad windows, and other slow-loading or intrusive content.</p> <p>See "Blocking Internet advertisements" on page 185.</p>

Alert Assistant	<p>The Alert Assistant helps you understand security issues, suggests how you can resolve problems, and advises you on avoiding future security problems.</p> <p>See "Learn more with the Alert Assistant" on page 61.</p>
Norton AntiSpam	<p>Norton AntiSpam helps reduce the amount of unwanted email messages that you receive by intelligently filtering incoming messages and clearly marking potential spam.</p> <p>See "Blocking unwanted email messages" on page 181.</p>
User Access Manager	<p>With the User Access Manager, network administrators can create user accounts, modify protection, and set program options for several computers at once.</p> <p>See "Transfer security settings to other computers" on page 75.</p>
Productivity Control	<p>Productivity Control lets administrators choose the Web sites and newsgroups that each user can visit and the types of Internet programs that users can access.</p> <p>See "Controlling individuals' Internet use" on page 165.</p>

Norton AntiSpam features

As email becomes more popular, many users are receiving an increasing amount of the unsolicited commercial email messages known as spam. Not only does spam make it difficult to identify valid email messages, some spam contains offensive messages and images.

Also, many Web sites are using more aggressive techniques to draw attention to the ads on their pages. Some have begun using larger, more prominent ads, while others rely on ad windows that appear when you enter or leave the site. Along with increasing the amount of time that it takes to display Web pages, some ads contain offensive content, cause software conflicts, or use [HTML](#) tricks to open additional browser windows.

Norton AntiSpam incorporates several powerful features to reduce your exposure to unwanted online content.

Automatic integration with email programs	<p>Automatically creates a toolbar in supported email programs</p> <p>See "Use your email program toolbar" on page 57.</p>
Allowed and Blocked lists	<ul style="list-style-type: none"> ■ Uses user-defined address list to expedite scanning of email ■ Accepts all mail from Allowed list ■ Treats all mail from Blocked list as spam <p>See "Manage how Norton AntiSpam detects spam" on page 66.</p>
Simplified import of addresses	<ul style="list-style-type: none"> ■ Imports lists of addresses from supported email programs ■ Allows all or selected addresses to be imported <p>See "Identify authorized senders" on page 67.</p>
Self-training	<p>Uses outgoing mail to refine spam definition</p> <p>See "Teach Norton AntiSpam your email preferences" on page 69.</p>

Custom spam rules	Lets you identify email addresses and text that should and should not be filtered See "Customize Norton AntiSpam" on page 181.
Ad blocking	Blocks ads based on user-defined criteria See "Blocking Internet advertisements" on page 185.
Popup blocking	Blocks pop-up windows based on user-defined criteria See "Enable or disable Popup Window Blocking" on page 72.
Live update of spam definitions	Updates copies of Symantec spam definition files automatically (subscription required) See "Keeping current with LiveUpdate" on page 103.

Virus and threat protection features

Norton AntiVirus provides comprehensive virus prevention, threat detection, and repair software for your computer. It automatically detects and repairs known viruses. Norton AntiVirus detects viruses and other potential risks in instant messenger attachments as well as in email messages, Internet downloads, and other files. Easy updating of the [virus definitions](#) over the Internet keeps Norton AntiVirus prepared for the latest [threats](#).

Norton AntiVirus now includes expanded threat detection of both known and emerging threats, such as spyware and other files that could put your computer at risk. Norton AntiVirus also scans files inside of compressed files.

As always, Norton AntiVirus features continually monitor your computer and protect it from known and unknown threats.

Feature	Description
Auto-Protect	<ul style="list-style-type: none"> ■ Loads into memory when Windows starts, providing constant protection while you work. ■ Checks for viruses every time that you use software programs on your computer, insert floppy disks or other removable media, access the Internet, or use document files that you receive or create. ■ Monitors your computer for any unusual symptoms that may indicate an active threat. <p>See "What to do if a virus is found" on page 145.</p>
Virus protection updates	<p>Updates your virus definitions automatically.</p> <p>See "About protection updates" on page 104.</p>
Compressed file protection	<p>Detects and repairs viruses inside of compressed files.</p> <p>See "What to do if a virus is found" on page 145.</p>

Feature	Description
Email protection	<p>Protects incoming and outgoing email messages, preventing your computer and other computers from infection.</p> <p>See "What to do if a virus is found" on page 145.</p>
Instant messenger protection	<p>Scans for and detects viruses in instant messenger attachments.</p> <p>See "What to do if a virus is found" on page 145.</p>
Bloodhound technology	<p>Detects new and unknown viruses by analyzing an executable file's structure, behavior, and other attributes such as programming logic, computer instructions, and any data that is contained in the file.</p> <p>See "What to do if a virus is found" on page 145.</p>
Password protection	<p>Protects Norton AntiVirus options from unauthorized changes.</p> <p>See "Password protect Norton AntiVirus options" on page 101.</p>

Advanced Utilities features

Norton Utilities keeps your computer working its best by finding, solving, and preventing Windows and disk problems. The UnErase and Wipe Info tools include the following features:

UnErase Wizard (Windows 98/Me/ 2000/XP)	Locates and recovers files that are protected by Norton Protection or the Windows Recycle Bin. See "About UnErase Wizard" on page 190.
Norton Protection (Windows 98/Me/ 2000/XP)	Adds extra data recovery protection to the Recycle Bin. When used in conjunction with UnErase Wizard, it provides the most complete recovery system for all deleted or overwritten files. See "About Norton Protection" on page 189.
Wipe Info (Windows 98/Me/ 2000/XP)	Permanently removes unwanted files so that they never can be recovered by a file recovery program. It can also wipe the free space on your hard disk, to ensure that previously deleted information is not left on your hard disk. See "Eliminating data permanently" on page 193.

Web Tools features

With Web Tools you can delete unneeded files that have accumulated during Internet sessions, including cookies, cache files, and Internet history files. You can also prevent interruption during dial-up Internet sessions. Web Tools include the following features:

Web Cleanup	Scans your computer for unnecessary files that have been left on your computer after you browse the Internet with Internet Explorer. You can delete these files or view them and decide which ones to keep. See "About Web Cleanup" on page 199.
Connection Keep Alive	Helps maintain your dial-up connection to the Internet, even when your computer is idle. See "About Connection Keep Alive" on page 205.

Installing Norton Internet Security Professional

3

Before installing Norton Internet Security Professional, take a moment to review the system requirements. Windows 98/Me users should have several blank 1.44-MB disks available to make Rescue Disks.

System requirements

To use Norton Internet Security Professional, your computer must have one of the following Windows operating systems installed:

- Windows 98, 98SE
- Windows Me
- Windows 2000 Professional
- Windows XP Professional/Home Edition

Windows 95 and NT, the server editions of Windows 2000/XP, and the Windows XP 64-bit edition are not supported.

Your computer must also meet the following minimum requirements.

Operating System	Requirements
Windows 98/98SE	<ul style="list-style-type: none"> ■ 133 MHz or higher processor ■ 64 MB of RAM ■ 200 MB of available hard disk space ■ Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended) ■ CD-ROM or DVD-ROM drive
Windows Me	<ul style="list-style-type: none"> ■ 150 MHz or higher processor ■ 96 MB of RAM ■ 200 MB of available hard disk space ■ Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended) ■ CD-ROM or DVD-ROM drive
Windows 2000 Professional	<ul style="list-style-type: none"> ■ 133 MHz or higher processor ■ 96 MB of RAM ■ 200 MB of available hard disk space ■ Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended) ■ CD-ROM or DVD-ROM drive
Windows XP Professional or Home Edition	<ul style="list-style-type: none"> ■ 300 MHz or higher processor ■ 128 MB of RAM ■ 200 MB of available hard disk space ■ Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended) ■ CD-ROM or DVD-ROM drive

Supported email and instant messenger programs

Norton Internet Security Professional adds security features to the following email and instant messenger programs.

Feature	Supported programs
Norton AntiSpam integration	<ul style="list-style-type: none"> ■ Microsoft® Outlook® Express 5.5 and later ■ Microsoft Outlook 2000/XP ■ Eudora® 5.0 and later
Email scanning	<p>Any POP3-compatible program, including:</p> <ul style="list-style-type: none"> ■ Microsoft Outlook Express 4.0/5.X ■ Microsoft Outlook 97/98/2000/XP ■ Netscape Messenger 4.X, Netscape Mail 6.0 ■ Eudora Light 3.0, Eudora Pro 4.0, Eudora 5.0
Privacy Control instant messaging scanning	<ul style="list-style-type: none"> ■ AOL Instant Messenger, version 4.3 or later ■ Yahoo! Messenger, version 5.0 or later ■ MSN Messenger and Windows Messenger, version 4.6 or later
Norton AntiVirus instant messaging scanning	<ul style="list-style-type: none"> ■ AOL Instant Messenger, version 4.7 or later ■ Yahoo! Messenger, version 5.0 or later ■ MSN Messenger and Windows Messenger, version 3.6 or later

Compatibility with other software and hardware

Norton Internet Security Professional works well with Symantec pcAnywhere and most routers, Internet connection sharing programs, and popular VPNs.

Symantec pcAnywhere

See ["Change an existing firewall rule"](#) on page 120.

You should have no problems using Symantec pcAnywhere as either a client or host with Norton Internet Security Professional. For maximum protection,

if you run a Symantec pcAnywhere host, edit the rule to limit its use to only the computers with which you use it. Symantec pcAnywhere passwords are also necessary for maximum security.

Routers

Norton Internet Security Professional adds to the protection provided by the router. In some cases, you might want to reduce the protection provided by the router so that you can use programs like NetMeeting or MSN Messenger. Norton Internet Security Professional also provides features that might not be available with cable and DSL routers, such as privacy protection.

Internet connection sharing programs

For basic protection, install Norton Internet Security Professional on the gateway computer. For maximum protection against *Trojan horses* or other problem programs that initiate outbound communications, install Norton Internet Security Professional on all computers that share the connection. You must have a license for each copy of Norton Internet Security Professional you install.

Virtual Private Networks

Norton Internet Security Professional works with the following Virtual Private Networks (VPNs):

- Symantec Enterprise VPN
- Symantec VelociRaptor
- Nortel
- VPNremote
- PGP
- SecureRemote

With most VPNs, when the VPN client is active, you cannot see the Internet or other computers on your local network. You can only see what is available through the VPN server to which you are connected.

About encrypted email connections

Norton Internet Security Professional does not support email connections using Secure Sockets Layer. Secure Sockets Layer (SSL) is a Netscape protocol designed to provide secure communications on the Internet. If you use an SSL connection to access your email, you are not protected by Norton Internet Security Professional.

To send email messages through SSL layer connections, turn off Privacy Control and Norton AntiSpam. If you have installed Norton AntiVirus, you must also turn off incoming and outgoing email protection.

To send email through SSL

- 1 In the main window, click **Privacy Control**.
- 2 In the lower-right corner of the window, click **Turn Off**.
- 3 Repeat steps 2 and 3, selecting Norton AntiSpam in step 2.
- 4 In the Security Center, click **Options > Norton AntiVirus**.



If you set a password for Options, Norton Internet Security Professional asks you for the password before you can continue.

- 5 In the Options window, click **Email**.
- 6 Click **OK**.
- 7 Uncheck Scan incoming Email (recommended).
- 8 Uncheck Scan outgoing Email (recommended).
- 9 Resend your email.

Before installation

Before you install Norton Internet Security Professional, prepare your computer.

If you have purchased multiple copies of Norton Internet Security Professional for several computers, you should prepare each computer before installing. You can use the same set of Emergency Disks for all of the computers.

Prepare your computer

Quit all other Windows programs before installing Norton Internet Security Professional. Other active programs may interfere with the installation and reduce your protection.

If you have a recent version of Norton Internet Security Professional, Norton Internet Security, or Norton Personal Firewall, the installer can import and use your current security settings. If you have an older version of these products, the installer prompts you to remove the older version.

You must also uninstall any antivirus programs that are installed on your computer. For more information, see the user documentation that came with the programs.

If you're using Windows XP

Windows XP includes a firewall that can interfere with Norton Internet Security Professional protection features. You must disable the Windows XP firewall before installing Norton Internet Security Professional.

To disable the Windows XP firewall

- 1 On the Windows XP taskbar, click **Start > Control Panel**.
- 2 In the Control Panel window, do one of the following:
 - In the default Category View, click **Network and Internet Connections**, then click **Network Connections**.
 - In the Classic View, double-click **Network Connections**.
- 3 Right-click the active connection icon, then click **Properties**.
- 4 In the Properties window, on the Advanced tab, uncheck **Protect my computer and network by limiting or preventing access to this computer from the Internet**.
- 5 Click **OK**.

Install Norton Internet Security Professional

You can install Norton Internet Security Professional from a CD or from a file you download. If you have not already done so, close all other Windows programs.

To install Norton Internet Security Professional

- 1 Do one of the following:
 - If you are installing from a CD, insert the CD into the CD-ROM drive.
 - If you downloaded your copy of Norton Internet Security Professional, double-click the file you downloaded, then click **Install**.
- 2 In the Norton Internet Security Professional window, click **Install Norton Internet Security Professional**.
- 3 In the Scan for Viruses dialog box, click **Yes** to scan your computer before installing.
- 4 In the Symantec Pre-Install Scanner window, review the progress of the scan.
If Norton AntiVirus detects a virus, it prompts you to delete each file individually.
- 5 Click **Delete** for each file.
- 6 After the scan completes, view the results in the scanresults-Notepad window.

See "If the opening screen does not appear" on page 46.

- 7 After you review the results, close the scanresults-Notepad window, then click **Next** to continue with the installation.



- 8 Read the License Agreement, then click **I accept the License Agreement**.
If you decline, you cannot continue with the installation.

9 Click **Next**.



See "When to activate your product" on page 26.

10 In the text boxes, type the product key for activation.

11 Click **Next**.



- 12 Select an installation type. Your options are:

Install Now	Install using the most common settings. This is the best choice for most users.
Custom	View a list of the components and programs that will be installed, and add or remove components from the list. See "Customize your installation" on page 45.

- 13 Click **Browse** to select a folder into which you want to install Norton Internet Security Professional, if it is other than the default location.
- 14 Click **Next**.



- 15 Confirm the installation location, then click **Next** to install Norton Internet Security Professional. The Norton Internet Security Professional Setup window displays installation progress. Depending on your computer system speed, this can take a few minutes.

- 16 After Norton Internet Security Professional is installed, read the readme text, then click **Next**.
- 17 Do one of the following:
 - To restart your computer now, click **Restart Now (recommended)**.
 - To restart your computer later, click **Restart Later**.Your computer is not protected until you restart.
- 18 Click **Finish**.

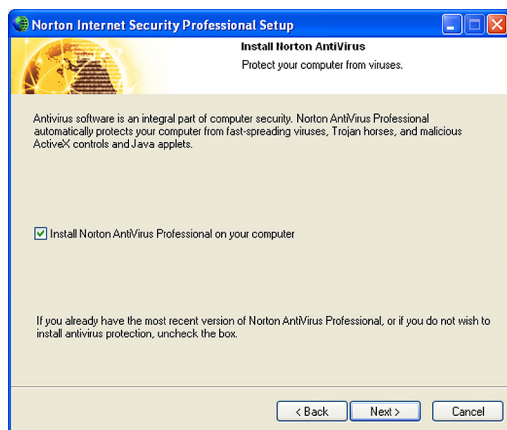
Customize your installation

During installation, if you select the Custom installation type, you can select the component programs that you want to install.

To customize your installation

See “Install Norton Internet Security Professional” on page 41.

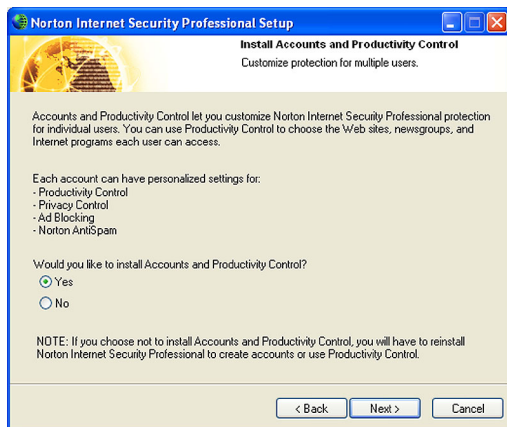
- 1 Start the Norton Internet Security Professional installation procedure.



- 2 To install Norton AntiVirus Professional, check **Install Norton AntiVirus Professional on your computer**.

If an updated version of Norton AntiVirus is already on your computer, this window does not appear.

3 Click **Next.**



- 4** In the Install Accounts and Productivity Control window, select whether you want to install Accounts and Productivity Control.
If you do not install these features, you will have to reinstall Norton Internet Security Professional to create accounts or use Productivity Control.
- 5** Click **Next** to continue the installation at the confirm the installation location step.

See ["Install Norton Internet Security Professional"](#) on page 41.

If the opening screen does not appear

Sometimes a computer's CD-ROM drive does not automatically run a CD.

To start the installation from the Norton Internet Security Professional CD

- 1 On your desktop, double-click **My Computer**.
- 2 In the My Computer window, double-click the icon for your CD-ROM drive.
- 3 In the list of files, double-click **Cdstart.exe**.

After installation

After Norton Internet Security Professional is installed and you have restarted your computer, the Information Wizard appears.

Use the Information Wizard

The Information Wizard lets you activate your copy of Norton Internet Security Professional, get information about updates, select post-installation tasks to be done automatically, and review your security settings.



If you choose not to register the software using the Information Wizard or if registration fails for some reason, you can register by using the Product Registration option on the Help menu or by using the Symantec Web site at www.symantec.com. On the Web site, go to the Products page for the registration link.

To use the Information Wizard

- 1 In the welcome window, click **Next**.



You must activate the software within 15 days.

- 2 On the Product Activation window, click **Activate and register your product now**.
- 3 Click **Next**.
- 4 Make sure that your computer is connected to the Internet, then click **Next**.
- 5 If you purchased your computer with Norton Internet Security Professional already installed, you must accept the license agreement in order to use Norton Internet Security Professional. Click **I accept the license agreement**, then click **Next**.

See "When to activate your product" on page 26.

- 6
- In the first Registration window, select the Country/Region from which you are registering.
- 7
- If you would like information from Symantec about Norton Internet Security Professional, check the method by which you want to receive that information, type the corresponding address and phone number, then click **Next**.
- 8
- Check if you would like to receive postal mail from Symantec.
- 9
- Type your name and address, then click **Next**.
- 10
- Make sure your computer is connected to the Internet, then click **Next** to activate.
- 11
- Click **Finish**.
- 12
- Select the post-installation tasks that you want Norton Internet Security Professional to perform automatically. Your options are:

Import your email address book	Quickly add the people in your email address book to your Allowed List. See "Identify authorized senders" on page 67.
Scan for Viruses	Perform a full system scan. See "Manually scan disks, folders, and files" on page 136.
Set up Privacy Control	Identify the information you want Privacy Control to protect. See "Identify private information to protect" on page 175.
Set up Productivity Control	Create accounts for individual users. See "Create Norton Internet Security Professional accounts" on page 157.
Run LiveUpdate	Ensure that you have the latest security updates. See "Keeping current with LiveUpdate" on page 103.

13 Click **Next**.

14 Review the post-installation tasks and configuration settings for Norton Internet Security Professional. If you want to change any of the settings, do so using Options.

15 Click **Finish**.

If you selected any post-installation tasks, they start automatically.



If you need to uninstall Norton Internet Security Professional

If you need to remove Norton Internet Security Professional from your computer, use the Add/Remove Programs option from the Windows Control Panel. You can also uninstall only the Norton AntiVirus component of Norton Internet Security Professional.



During uninstallation, Windows may indicate that it is installing software. This is a standard Microsoft installation message and can be disregarded.

To uninstall Norton Internet Security Professional

- 1 Do one of the following:
 - On the Windows taskbar, click **Start > Settings > Control Panel**.
 - On the Windows XP taskbar, click **Start > Control Panel**.
- 2 In the Control Panel, double-click **Add/Remove Programs**.
- 3 In the list of currently installed programs, click **Norton Internet Security Professional**.
- 4 Do one of the following:
 - In Windows 2000/Me, click **Change/Remove**.
 - In Windows 98, click **Add/Remove**.
 - In Windows XP, click **Change**.
- 5 Do one of the following:
 - Click **Remove NAV** to uninstall the Norton AntiVirus component of Norton Internet Security Professional.
 - Click **Remove All** to uninstall the entire product.
- 6 If you plan to reinstall Norton Internet Security Professional, check **Save my settings**. This saves a copy of your current security settings. You can then import these settings to restore your protection.
- 7 Click **Next**.

- 8 If you have files in Quarantine, you are asked if you want to delete them. Your options are:

Yes	Deletes the quarantined files from your computer
No	Leaves the quarantined files on your computer, but makes them inaccessible

- 9 Click **Next**.

- 10 In the Norton Internet Security Professional has been successfully removed window, do one of the following:

- To restart your computer now, click **Restart Now (recommended)**.
- To restart your computer later, click **Restart Later**.

Norton Internet Security Professional is not fully uninstalled until you restart your computer.

- 11 Click **Finish**.



Basics include general information about how to:

- Work with your Symantec product.
- Keep your computer protected.
- Customize options.
- Monitor protection activities.
- Access more information.

Check the version number

You can check the version number of your product on your computer. Use the version number to help you find more information about your product on the Symantec Web site.

To check the version number

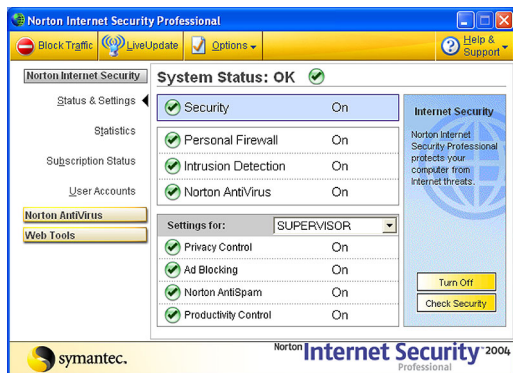
- 1 Start your product.
- 2 Click **Help and Support**.
- 3 On the Help menu, click **About <your product name>**.
- 4 In the About dialog box, select your product name.

Start Norton Internet Security Professional

After installation, Norton Internet Security Professional automatically protects any computer on which it is installed. You do not have to start the program to be protected.

To start Norton Internet Security Professional

- ❖ Do one of the following:
 - On the Windows taskbar, click **Start > Programs > Norton Internet Security Professional > Norton Internet Security Professional**.
 - On the Windows XP taskbar, click **Start > All Programs > Norton Internet Security Professional > Norton Internet Security Professional**.
 - On the Windows desktop, double-click **Norton Internet Security Professional**.



Use the Norton Internet Security Professional tray icon

Norton Internet Security Professional adds an icon to the Windows system tray at the end of the Windows taskbar. Use this icon as a shortcut to open Norton Internet Security Professional, block all Internet traffic, turn off all Norton Internet Security Professional protection features, and learn more about Norton Internet Security Professional.

See ["About General options"](#) on page 93.

You can also use the Norton Internet Security Professional Options to add additional tools to the menu.

To use the Norton Internet Security Professional tray icon

- 1 In the Windows system tray, right-click the Norton Internet Security Professional icon.
- 2 On the tray icon menu, select the option you want. Your options are:

Norton Internet Security Professional	Opens the Norton Internet Security Professional main window
Block Traffic	Immediately stops all Internet communication
Log Off	Logs off the current user
About Norton Internet Security Professional	Displays more information about Norton Internet Security Professional
LiveUpdate	Lets you update your protection
Help	Opens the online Help
Disable	Stops Norton Internet Security Professional from protecting your computer

Use Web assistant from the Internet Explorer toolbar

See ["Use Web assistant"](#) on page 62.

Norton Internet Security Professional now includes Web assistant, which lets you quickly access security settings without leaving your Web browser.



Use your email program toolbar

Norton AntiSpam adds a button or buttons to the toolbar of supported email programs. If a single Norton AntiSpam button is added, it drops down an abbreviated Norton AntiSpam menu. The buttons or menu options added are as follows:

This is Spam	Marks the selected email as spam
This is not Spam	Marks the selected email as allowed (not spam)
Empty The Spam Folder	Removes all email that has been placed in the Norton AntiSpam folder
Open Norton AntiSpam	Displays the Norton AntiSpam main window

Start Norton AntiVirus

After installation, Norton AntiVirus automatically protects any computer on which it is installed. You do not have to start the program to be protected.

To start Norton AntiVirus

- ❖ Do one of the following:
 - On the Windows taskbar, click **Start > Programs > Norton AntiVirus > Norton AntiVirus 2004**.
 - On the Windows XP taskbar, click **Start > More Programs > Norton AntiVirus > Norton AntiVirus 2004**.
 - On the desktop, double-click the Norton Internet Security Professional icon.

Use the Norton AntiVirus icon in the Windows system tray

See ["Customize Norton AntiVirus"](#) on page 96.

Norton AntiVirus adds an icon to the Windows system tray at the end of the Windows taskbar. Use the icon in the Windows system tray to open Norton AntiVirus and to enable or disable Auto-Protect.

To use the Norton AntiVirus Windows system tray icon

- ❖ In the Windows system tray, right-click the Norton AntiVirus icon, then on the tray icon menu, select the option that you want.

Use the Windows Explorer toolbar

Norton AntiVirus adds a button and menu to Windows Explorer.

When you first open Windows Explorer after installing Norton AntiVirus, you may not see the Norton AntiVirus button and menu. You might have to restart Windows before the toolbar button appears.



You may not be able to access the Norton AntiVirus Windows Explorer menu, depending on your computer's configuration.

To display the Norton AntiVirus button and menu

- 1 On the View menu, click **Toolbars > Norton AntiVirus**.
- 2 Click the arrow to the right of the button to view your options. Your options are:

View Status	Launches Norton AntiVirus and displays the Status window with system status. See " Check Norton AntiVirus configuration status " on page 73.
View Quarantine	Displays the Quarantine area and the files currently stored there. See " If Norton AntiVirus places files in Quarantine " on page 152.
View Activity Log	Displays the Log Viewer, which shows you various Norton AntiVirus activities, such as scans performed and problems found. See " Monitor Norton AntiVirus activities " on page 214.
View Virus Encyclopedia	Connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.
Launch Scan Menu	Opens Norton AntiVirus in the Scan for Viruses pane, on which you can specify a scan to run.

Activate your product



Product activation reduces software piracy and ensures that you have received genuine Symantec software.

You must activate your product within 15 days of installing it or the product will stop working.

If you did not activate your product using the Configuration Wizard, you will receive an Activation Needed *alert* every day until you activate the product.

You can activate your product from the Activation Needed alert or from the Activation option on the Help menu. Activation should take just a few minutes.

To activate your product from the Activation Needed alert

- 1 In the alert, click **Activate Now**.
- 2 Click **OK**.
- 3 On the Activation screen, click **Next**.
- 4 On the Activation Successful screen, click **Finish**.

To activate your product from the Help menu

- 1 At the top of the main window, click **Help and Support > Activation**.
- 2 On the Activation screen, click **Next**.
- 3 On the Activation Successful screen, click **Finish**.

Respond to Norton Internet Security Professional alerts



When a Norton Internet Security Professional [alert](#) appears, read it before you make a decision. Identify what type of alert it is and the threat level. Once you understand the risks, you can make a choice.

Take as much time as you need to make your choice. Your computer is safe from attack while the alert is active.

Norton Internet Security Professional helps you decide on an appropriate action by preselecting the recommended action if one exists. Norton Internet Security Professional cannot suggest recommended actions for all alerts.

See "[Customizing protection for different locations](#)" on page 129.

The first alert most people will receive is a New Location Alert. This alert appears every time your computer joins a network that Network Detector does not recognize. You will likely receive a New Location Alert the first time you go online after installing Norton Internet Security Professional.

Learn more with the Alert Assistant

Each Norton Internet Security Professional [alert](#) includes a link to the Alert Assistant. The Alert Assistant includes customized information about each alert, including:

- The type of alert
- The threat level
- The communication that triggered this alert
- What these types of alerts indicate
- How to reduce the number of these alerts you receive

To use the Alert Assistant

- 1 In any alert, click **Alert Assistant**.
- 2 In the Alert Assistant window, review the information about the alert.
- 3 To respond to the alert, close the Alert Assistant.

Use Web assistant

Web assistant lets you customize Ad Blocking and Privacy Control settings for individual Web sites without leaving your browser. Web assistant adds a button to your Microsoft Internet Explorer toolbar that gives you fast access to Ad Blocking, Privacy Control, and the Norton Internet Security Professional main window.

The Web assistant menu includes the following tasks.

Block cookies on this site	Prevents this site from setting or reading cookie files
Block ads on this site	Removes ad images from pages on this site
Block popups on this site	Prevents this site from opening unrequested browser windows
Open Ad Trashcan	Opens the Ad Trashcan, which lets you choose the ads you want to block
Configure security settings	Opens the main Norton Internet Security Professional window

After installing Norton Internet Security Professional, the Web assistant button appears in your Internet Explorer toolbar. If you have locked your toolbars, the Web assistant button may be hidden.

To view or hide Web assistant

- ❖ In Microsoft Internet Explorer, right-click the toolbar, then click **Web assistant**.

Check your computer's vulnerability to attack

Use Security Check to test your computer's vulnerability to security intrusions. The Security Check link in Norton Internet Security Professional connects you to the

Identify the source of Internet traffic

Symantec Web site, where you can scan for vulnerabilities and get detailed information about Security Check scans.



You must be connected to the Internet to check your computer's vulnerability.

To check your computer's vulnerability to attack

- 1 In the main window, click **Security**.
- 2 Click **Check Security**.
- 3 On the Security Check Web page, click **Scan for Security Risks**.
- 4 To learn more about the Security Check tests, click **About Scan for Security Risks**.

When the scan is complete, the results page lists all of the areas that were checked and your level of vulnerability in each one. For any area marked as at risk, you can get more details about the problem and how to fix it.

To get more information about an at-risk area

- ❖ On the results page, next to the scan name, click **Show Details**.

Identify the source of Internet traffic

Visual Tracking helps you learn more about computers that attempt to connect to your computer. Using Visual Tracking, you can identify the location of the [IP address](#) used and contact information for the owner of the address. You can use this information to identify the origin of an attack and to learn more about intrusion attempts.

You can trace connection attempts from the following locations:

- Statistics window
- AutoBlock
- Alerts

Stop all Internet communication

When Visual Tracking is finished, it displays a visual representation of where this communication originated and contact information for the owner of the IP address.

To trace a connection attempt from the Statistics window

- 1 In the main window, click **Statistics**.
- 2 Click **Attacker Details**.
Your browser opens the Visual Tracking Web page.

To trace a connection attempt from AutoBlock

- 1 In the main window, double-click **Intrusion Detection**.
- 2 In the Intrusion Detection window, under AutoBlock, select a connection you want to trace.
- 3 Click **Attacker Details**.
Your browser opens the Visual Tracking Web page.

To trace a connection attempt from the Alert Assistant

- 1 In a security alert, click **Alert Assistant**.
- 2 Click the IP address of the attacking computer.
Your browser opens the Visual Tracking Web page.

Stop all Internet communication

Block Traffic lets you immediately halt any communication between your computer and another. This can be a convenient way to limit any damage to your computer if it is attacked, if a *Trojan horse* is sending personal information without your permission, or if you inadvertently allow an untrusted person to access files on your computer.

When this option is active, Norton Internet Security Professional stops all communication to and from your computer. To the outside world, it appears that your computer has completely disconnected from the Internet.

If you want to block all traffic into and out of your computer, Block Traffic is more effective than simply using your Internet software to disconnect. Most Internet programs can automatically connect without any input

from the user, so a malicious program could reconnect when you are away from the computer.



Block Traffic is meant to be used as a temporary measure while you address a security problem. If you restart your computer, Norton Internet Security Professional automatically allows all incoming and outgoing communication.

To stop all Internet communication using Block Traffic

- 1** In the main window, click **Block Traffic**.
- 2** Use Norton Internet Security Professional tools to address the security problem.
- 3** When you have fixed the problem, click **Allow Traffic**.

Manage how Norton AntiSpam detects spam

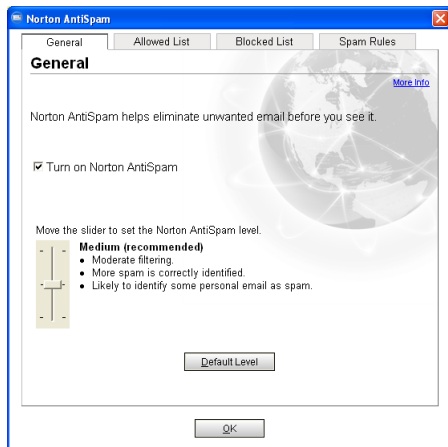
Norton AntiSpam begins filtering email as soon as it is installed. If you are using a supported email program, it will also be available from within that program after installation.

Adjust the email filter

You can determine how strictly Norton AntiSpam filters your email. Adjust the Norton AntiSpam parameters from the main window.

To adjust the email filter

- 1 In the main window, double-click **AntiSpam**.
- 2 In the Norton AntiSpam window, in the Norton AntiSpam settings for drop-down list, select the account that you want to change.



- 3 In the General window, ensure that Turn on Norton AntiSpam is checked.

Manage how Norton AntiSpam detects spam

- 4 Use the Norton AntiSpam slider to control how Norton AntiSpam filters email. Your options are:

High	Maximum filtering. Most spam is correctly identified. More likely to identify personal email messages as spam.
Medium (recommended)	Moderate filtering. More spam is correctly identified. Likely to identify some personal email messages as spam.
Low	Light filtering. Some spam is correctly identified. Rarely identifies personal email messages as spam.

- 5 Click **OK**.

Identify authorized senders

To tell Norton AntiSpam that you want to receive email from a given address, add it to the Allowed list.

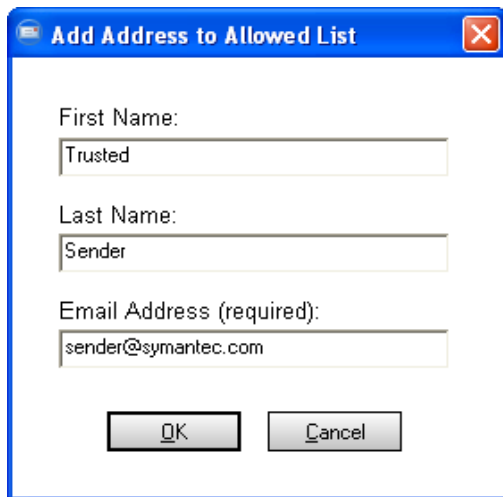
If you did not import your email address book to your Allowed list during installation, you can do so at any time after installation. You can import some or all of the addresses. You can also add names to the Allowed list individually.

To import your existing address book

- 1 In the main window, double-click **Allowed List**.
- 2 In the Allowed List window, click **Import Address Book**.
- 3 In the Import Address Book window, uncheck any addresses that you do not want to add to your Allowed list.
- 4 Click **OK**.
- 5 Click **OK** to close the Allowed List window.

To add names to your allowed list

- 1 In the main window, double-click **Allowed List**.
- 2 In the Allowed List window, click **Add**.



Add Address to Allowed List

First Name:
Trusted

Last Name:
Sender

Email Address (required):
sender@symantec.com

OK Cancel

- 3 In the Add Address to Allowed List dialog box, type the email address you want to allow and, optionally, the first and last name of the sender.
- 4 Click **OK** to close the Add Address to Allowed List dialog box.
- 5 Click **OK** to close the Allowed List window.

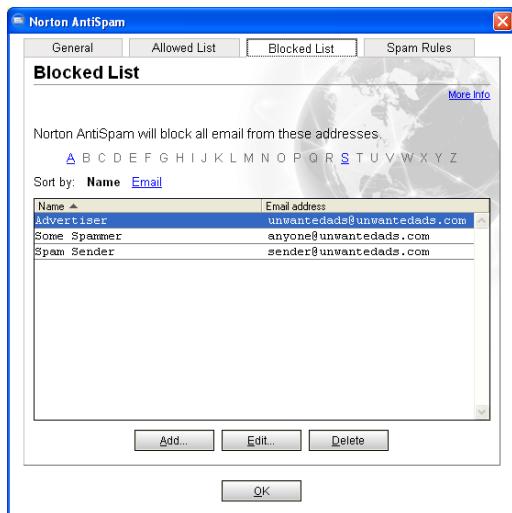
Identify senders of spam email messages

When you know that you do not want to receive any email messages from a specific address, you can add it to the Blocked List. Norton AntiSpam will mark all email messages from this address as spam.

Manage how Norton AntiSpam detects spam

To add names to the Blocked List

- 1 In the main window, double-click **Blocked List**.



- 2 In the Blocked List window, click **Add**.
- 3 In the Add Address to Blocked List dialog box, type the email address you want to block and, optionally, the first and last name of the sender.
- 4 Click **OK** to close the Add Address to Blocked List dialog box.
- 5 Click **OK** to close the Blocked List window.

Teach Norton AntiSpam your email preferences

Norton AntiSpam's filtering engine attempts to identify spam automatically by using your outgoing email to determine your usual email correspondents. Over time, you can train Norton AntiSpam to reflect your personal preferences for receiving email more precisely.

To train the filtering engine

- 1 Start your email program.
- 2 Select each item that should have been marked as spam.
- 3 Using the buttons added to your email program by Norton AntiSpam, click **This is Spam**.
- 4 If you have set your options to ask before adding senders to the Blocked List, answer the prompt accordingly.
- 5 Open the **Norton AntiSpam** folder.
- 6 Select each item that should not have been marked as spam.
- 7 Using the buttons added to your email program by Norton AntiSpam, click **This is not Spam**.
- 8 If you have set your options to ask before adding senders to the Allowed List, answer the prompt accordingly.
- 9 Close your email program.

Manage advertising filters

Ad Blocking can block several kinds of ads that appear on Web sites while you are browsing the Internet.

You can set individual Ad Blocking settings for each user. Supervisor and Standard users can make changes to program settings. Restricted users cannot make any changes to Ad Blocking.

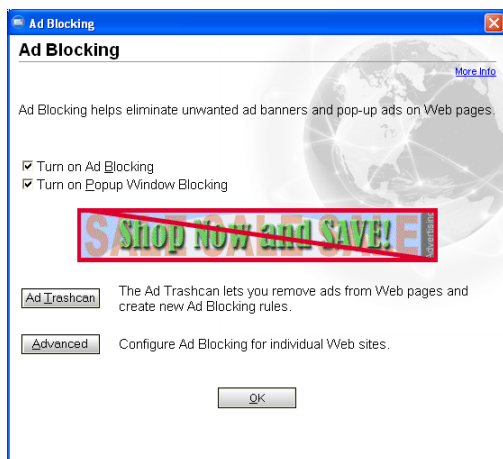
Enable or disable Ad Blocking

Ad Blocking compares the addresses of ads that are being downloaded by your browser with its own list of ads to block. If it finds a match, it removes the ad so that it does not appear in your browser, leaving the rest of the Web page intact.

Sometimes you may want to view ads that have been blocked. In this case, you can temporarily disable Ad Blocking.

To enable or disable Ad Blocking

- 1 In the main window, double-click **Ad Blocking**.



- 2 In the Ad Blocking window, check or uncheck **Turn on Ad Blocking**.
- 3 Click **OK**.

Enable or disable Popup Window Blocking

Pop-up and pop-under ads are secondary windows that Web sites open when you visit or leave the sites. Pop-ups appear on top of the current window, while pop-under ads appear behind the current window.

When Popup Window Blocking is enabled, Ad Blocking automatically blocks the programming code Web sites use to open secondary windows without your knowledge. Sites that open secondary windows when you click a link or perform other actions are not affected.

In some cases, you may want to view pop-up windows on a site. In this case, you can temporarily disable Popup Window Blocking.

To enable or disable Popup Window Blocking

- 1 In the main window, double-click **Ad Blocking**.
- 2 In the Ad Blocking window, check or uncheck **Turn on Popup Window Blocking**.
- 3 Click **OK**.

Check Norton AntiVirus configuration status

If Norton AntiVirus is behaving in an unexpected way, or if you're not sure that everything is being scanned for viruses, check the status on the main window.

In the System Status pane of the Norton AntiVirus main window, a check mark indicates that the system status is OK and a triangle indicates that your system needs attention. If you see a triangle, review the features to see which area needs attention.

If you see an exclamation point, it indicates that your subscription is either expired or your virus definitions are more than two weeks old. If your subscription is expired, renew it to maintain your protection. If your subscription is current, then you need to update your virus definitions.

See ["Customize Norton AntiVirus"](#) on page 96.

If you need to adjust any settings, use Options.

To check system status

- 1 In the main window, under Norton AntiVirus, click **Status**.
- 2 In the System Status pane, review the status to the right of each feature.
- 3 For information about a particular feature, select the feature.
The right pane displays a description and a link to more information about the feature.

Check Office Plug-in status

Office Plug-in protects Microsoft Office documents from viruses, worms, and virus-like activities. It scans documents whenever you open them in a Microsoft Office program. Office Plug-in is enabled in Options.



If you have set a password for Options, Norton AntiVirus asks you for the password before you can view or adjust the settings.

Check Norton AntiVirus configuration status**To check Office Plug-in status**

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the left pane of the Options window, under Other, click **Miscellaneous**.
- 3 Verify that Office Plug-in is enabled.

Transfer security settings to other computers

To ensure complete protection for your network, all computers must have Norton Internet Security Professional installed and properly configured.

You can manually set up each computer, or you can use the User Access Manager to configure program options, firewall rules, and other preferences on an administrator's computer, then export these settings to other computers. This is a quick and easy way to ensure that all computers in your office have the same level of protection.



Supervisor and Standard users can make changes to security settings after you set up their computers. This can result in inconsistent protection if a user makes a firewall rule too permissive or removes an important Privacy Control entry. For maximum security, you should create Restricted accounts only.

Configure settings

To export settings to other computers, you must first configure your own computer. The settings file is an exact copy of your computer's configuration that can be used to set up new computers quickly.



Settings files do not contain Norton AntiVirus, Web Tools, WipeInfo, or UnErase settings. You must configure each computer's antivirus settings manually.

Before exporting settings, check that you have properly configured the following settings.

Setting	More information
Program options	See "Set Norton Internet Security Professional options" on page 92.
User accounts	See "Creating accounts for multiple users" on page 155.
Personal Firewall	See "Customize firewall protection" on page 112.

Transfer security settings to other computers

Setting	More information
Automatic Program Control	See "Enable Automatic Program Control" on page 116.
Intrusion Detection	See "Customize Intrusion Detection" on page 124.
Privacy Control	See "Protecting your privacy" on page 175.

For maximum security, you may want to create a special administrator account that is used only to export and import settings files. This ensures that you do not accidentally make unwanted changes to the master settings file if you have to customize Norton Internet Security Professional to accommodate any special requirements that you may have.

If you're using Windows accounts with Norton Internet Security Professional

If you chose to use Windows accounts instead of creating Norton Internet Security Professional accounts, the Windows accounts must exist on the administrator's computer and the computers to which you are transferring settings.

See ["Creating accounts for multiple users"](#) on page 155.

If users attempt to use Windows accounts that do not exist on the administrator's computer, Norton Internet Security Professional will use the Not Logged In settings and block all connection attempts. To learn how to create new Windows accounts, refer to your Windows documentation.

Export the settings file

When you have configured your copy of Norton Internet Security Professional, export the configuration to a settings file.

Use the Norton Internet Security Professional options to export settings information into a settings file. This file is encrypted and password-protected.

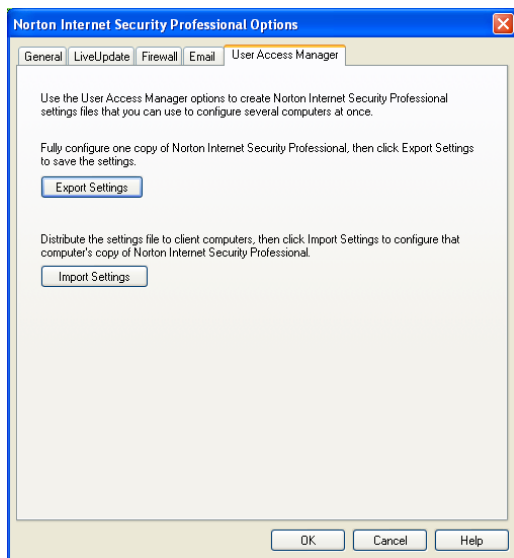
Transfer security settings to other computers



You must be logged on as a Supervisor user to export settings files.

To export a settings file

- 1 At the top of the main window, click **Options > Internet Security**.



- 2 In the Options window, on the **User Access Manager** tab, click **Export Settings**.
- 3 In the Save As window, select a location and name for the exported settings file.
 - If the computers in your office are networked, you can save the settings file on the administrator's computer or a central server, then use file sharing to connect and download the file to other computers.
 - If your computers are not networked, copy the settings file onto a floppy disk or other portable storage and distribute it.

Transfer security settings to other computers

- 4 In the Password window, type a password for the settings file.
Make note of the password. You must type it when importing the settings file.
- 5 Click **OK**.

Import the settings file

After exporting a settings file, use the Norton Internet Security Professional options to import settings files. Importing a settings file overwrites any changes that the computer's users have made.



You must be logged on as a Supervisor user to import settings files.

To import a settings file

- 1 On the computer on which you are importing settings, start Norton Internet Security Professional.
- 2 In the main window, click **Options > Internet Security**.
- 3 In the Options window, on the User Access Manager tab, click **Import Settings**.
- 4 In the Open window, select the settings file.
- 5 In the Password window, type the password that you set when exporting the file.
- 6 Click **OK**.
- 7 In the confirmation dialog box, click **OK**.
- 8 Click **Yes** to restart your computer and begin using the imported settings.

Temporarily disable Norton Internet Security Professional

See "About Norton Internet Security Professional accounts" on page 156.

There may be times when you want to temporarily disable Norton Internet Security Professional or one of its features. For example, you might want to see if Norton Internet Security Professional is preventing a Web page from appearing correctly.

Only Supervisor users can temporarily disable Norton Internet Security Professional. Restricted users cannot disable any portion of Norton Internet Security Professional.

Disabling Norton Internet Security Professional also disables all of the individual features.

To temporarily disable Norton Internet Security Professional

- 1 In the main window, click **Security**.
- 2 In the lower-right corner of the window, click **Turn Off**.

Norton Internet Security Professional is automatically turned back on the next time that you start your computer.

You can also disable individual security features. For example, you might want to see if the Personal Firewall is preventing a program from operating correctly.

To disable a protection feature

- 1 In the main window, select the feature that you want to disable.
- 2 In the lower-right corner of the window, click **Turn Off**.

Create and use Rescue Disks



Rescue Disks are available only for Windows 98/Me.

Rescue Disks are images on floppy disks that let you restart your computer when your hard disk is damaged or infected with a virus.

About Rescue Disks

Rescue Disks record a duplicate set of system startup files and disk partition information, and store rescue utilities, configuration files, and a DOS-based Norton AntiVirus scanner across multiple floppy disks or on a network drive.

You can customize your Rescue Disk set. It can consist of one *bootable* floppy disk, one Norton AntiVirus Program floppy disk, and at least six Virus Definition floppy disks. If you have Norton Utilities installed, you can also have two Norton Utilities floppy disks in your Rescue Disk set. With a Rescue Disk set, you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems.



Rescue Disks contain information specific to the computer on which they were made.

If you are using Rescue Disks for recovery, you must use the disks made for your computer.

If you are using Rescue Disks to scan for viruses, you can use disks made for a different computer.

You should update Rescue Disks whenever you update your virus protection, install new software, or make changes to your hardware.

See "If you need to use Rescue Disks to restore your system" on page 84.

Create a Rescue Disk set

You can create Rescue Disks any time. You can start the Rescue Disk Wizard from the main window of your Symantec product.

If you start the Rescue Disk Wizard from the main window, temporarily disable Auto-Protect while you are creating the Rescue Disk set. If you do not restart your computer after creating Rescue Disks, remember to enable Auto-Protect again.

When you select a floppy disk drive, the Rescue Disk program calculates the number of disks that you will need to complete the set. Depending on what items you want to include in the Rescue Disk set, you might need ten or more floppy disks.



If you choose to create Rescue Disks on a network drive, a second physical hard disk, or some other large capacity disk drive (but not a CD), your Rescue Disk set is placed in a folder on the selected disk. Make sure that you also have a bootable floppy disk in a safe location. This disk should contain the network *drivers* or other files necessary to start your computer and access the drive on which you placed your Rescue Disk set. Creating a Rescue Disk set on a startup hard disk, for example, drive C, is not recommended because you will not be able to access the rescue programs and configuration files if your hard disk is damaged and unable to start.

To create Rescue Disks

- 1 In the main window, click **Rescue**.
- 2 In the Rescue Disk window, select the drive on which to create the Rescue Disk set.
To create a Rescue Disk set on floppy disks, select drive A.
When you select a floppy disk drive, the Basic Rescue program displays the number of floppy disks that you will need to create the Rescue Disk set.
- 3 To make changes to the default Rescue Disk settings, click **Options** and do the following:
 - On the Rescue Files tab, specify the files to include in the Rescue Disk set. If you change the default file selection, the number of required floppy disks will also change.
 - On the Format Settings tab, select the type of format, if any, that you want Rescue Disk to use

when it prepares the bootable floppy disk for the Rescue Disk set.

- 4 Click **OK** to return to the Rescue Disk window.
- 5 When you have either assembled the required number of floppy disks or identified another location for the Rescue Disk files, click **Create**.
If you selected a floppy disk drive, Rescue Disk displays the Basic Rescue Disk List window and an estimate of how much time you will need to create the entire set.
- 6 Label the disks as specified in the Basic Rescue Disk List window, or type a descriptive name, then click **OK**.
Rescue Disk prompts you to insert the first disk in the floppy disk drive. If you selected a network drive or other larger-format drive, Rescue Disk prompts you for a Rescue Folder drive location.
- 7 Insert the disks as requested.
- 8 When you have finished creating the basic Rescue Disk set, in the Rescue Disk window, click **Close**.

Test your Rescue Disks

After you have created the Rescue Disk set, you are prompted to test your disks. This requires that you restart your computer using the Rescue Disks.



If you created Rescue Disks on a network drive, a second physical hard disk, or some other large capacity disk drive, you will have to restart into DOS from an external floppy disk, navigate to the Rescue folder, and run Rescue.exe.

To test your Rescue Disks

- 1 Close all open Windows programs.
- 2 Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A, then click **Restart**.
If the Rescue Disk screen appears on your monitor, the Rescue Disk works properly.
If the Rescue Disk screen does not appear, you have several options for correcting the problem.

See "My Rescue Disk does not work" on page 229.

- 3 Press **Escape** to exit to DOS.
- 4 Remove the disk from drive A and slide open the plastic tab on the back of the disk to write-protect it.
- 5 Restart your computer.

Update your Rescue Disks

You can update your Rescue Disks as often as you like. Rescue Disk lets you update your basic Rescue Disk set without having to recreate them.

If you are updating a floppy disk set, make sure that your disks are not write-protected before you begin.

To update your Rescue Disks


- 1 In the main window, click **Rescue**.
- 2 In the Rescue Disk window, under Select Destination Drive, click **drive A**, then click **Update**.
A message prompts you to insert the disk labeled Basic Rescue Boot Floppy Disk into drive A.
- 3 Insert the Basic Rescue Boot Floppy Disk into drive A, then click **OK**.
- 4 Insert the remaining disks in your set as requested.

Make sure to test your newly updated Rescue Disk set when prompted.

See [“Test your Rescue Disks”](#) on page 82.

Rescue Disk options

Rescue Disk has the following options.

Add Files	Click to specify additional files that you want Rescue Disk to store on the Rescue Disk set.
	 Do not use this as a backup utility. Add files only if they are needed to restore your system after a crash.
Remove File	Click to remove the selected file under User-selected Files. The files will no longer be included on the Rescue Disk set.

If you need to use Rescue Disks to restore your system

Rescue items list	<p>The list is categorized and presented in a hierarchical view, similar to a Windows Explorer view. Click the plus sign next to a category to expand the list and see what the category contains. Click the plus sign next to a specific file for more information about the file.</p> <p>The list of rescue items is different depending on the programs you have installed and the type of Rescue Disk set you are using.</p>
Basic Rescue Boot Floppy Files	Files that Rescue Disk stores on the floppy disk that you use to start your system.
Rescue DOS Utility Programs	DOS-based emergency programs that Rescue Disk stores on the Rescue Disk set. You can use these DOS-based utilities to recover your system.
Norton AntiVirus Program	Norton AntiVirus program files.
Definitions Disks	Virus definitions files used by Norton AntiVirus to scan your system in an emergency. There are several of these disks.
User-selected Files	Files you have added to the Rescue Disk set. Add files to this list by clicking Add Files. Remove files from this list by clicking the file, then clicking Remove File.

If you need to use Rescue Disks to restore your system



Rescue Disks are available only for Windows 98/Me.

Sometimes a virus or threat prevents your computer from starting normally. Some viruses can only be removed if the computer is started from a clean disk, not the infected hard disk. Often, a Norton AntiVirus *alert* tells you when to use your Rescue Disks.

If you need to use Rescue Disks to restore your system

You first need to determine if your Rescue Disks are current. This means that you have created or updated your Rescue Disks since you did any of the following:

- Added, modified, or removed internal hardware
- Added, modified, or removed hard disk partitions
- Upgraded your operating system
- Updated virus definitions

If your Rescue Disks are not current, you can still use them to remove viruses from your computer. When the Rescue Disk screen appears, use only the Norton AntiVirus task.

To use your Rescue Disks

- 1 Insert the Basic Rescue Boot Floppy Disk into drive A and restart your computer.
The Rescue program runs in DOS.
- 2 Use the arrow keys to select the program that you want to run.
A description of the selected program appears in the right pane of the Rescue program. Your options are:

Norton AntiVirus	Scans your computer for viruses and repairs any infected files
Rescue Recovery	Checks and restores boot and partition information

- 3 Press **Enter** to run the selected program.
- 4 Follow the on-screen instructions for inserting and removing the Rescue Disks.
- 5 When the Rescue program is done, remove the Rescue Disk from drive A and restart your computer.

For more information

The product documentation provides glossary terms, online Help, a Readme file, the User's Guide in PDF format, and links to the Knowledge Base on the Symantec Web site.

Look up glossary terms

Technical terms that are italicized in the User's Guide are defined in the glossary, which is available in both the User's Guide PDF and Help. In both locations, clicking a glossary term takes you to its definition.

Use online Help

Help is available throughout your Symantec product. Help buttons or links to more information provide information that is specific to the task that you are completing. The Help menu provides a comprehensive guide to all of the product features and tasks that you can complete.

To use online Help

- 1 At the top of the main window, click **Help & Support > Norton Internet Security Professional**.
- 2 In the Help window, in the left pane, select a tab. Your options are:

Contents	Displays the Help by topic
Index	Lists Help topics in alphabetical order by key word
Search	Opens a search field in which you can enter a word or phrase

Window and dialog box Help

Window and dialog box Help provides information about the program. This type of Help is context-sensitive, meaning that it provides help for the dialog box or window that you are currently using.

To access window or dialog box Help

- ❖ Do one of the following:
 - In the window, click any available Help link.
 - In the dialog box, click **Help**.

Readme file

The Readme file contains information about installation and compatibility issues. It also contains technical tips and information about product changes that occurred after this guide went to press. It is installed on your hard disk in the same location as the product files.

To read the Readme file

- 1 In Windows Explorer, double-click **My Computer**.
- 2 Double-click the hard disk on which you installed Norton Internet Security Professional.
In most cases, this will be drive C.
- 3 Click **Program Files > Norton Internet Security Professional**.
- 4 Double-click **Readme.txt**.
The file opens in Notepad or your default word processing program.
- 5 Close the word processing program when you are done reading the file.

Access the User's Guide PDF

The *Norton Internet Security Professional User's Guide* is provided on the CD in PDF format. You must have Adobe Acrobat Reader installed on your computer to read the PDF.



If you purchased this product as an electronic download, Adobe Acrobat Reader was not included. You must download it from the Adobe Web site.

To install Adobe Acrobat Reader

- 1 Insert the CD into the CD-ROM drive.
- 2 Click **Browse CD**.
- 3 In the CD window, double-click the **Manual** folder.
- 4 Double-click the program file.
- 5 Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

Once you have installed Adobe Acrobat Reader, you can read the PDF from the CD.



If you do not have a CD, you can download the PDF from the Symantec Service & Support Web site.

To read the User's Guide PDF from the CD

- 1 Insert the CD into the CD-ROM drive.
- 2 Click **Browse CD**.
- 3 Double-click the **Manual** folder.
- 4 Double-click **NIS.pdf**.

You can also copy a User's Guide to your hard disk and read it from there.

To read a User's Guide from your hard disk

- 1 Open the location into which you copied the PDF.
- 2 Double-click the PDF.

Symantec products on the Web

The Symantec Web site provides extensive information about all Symantec products. There are several ways to access the Symantec Web site.

To access the Web site from the Help menu

❖ Select the solution that you want. Your options are:

Symantec Security Response	Takes you to the Security Response page of the Symantec Web site, from which you can update your protection and read the latest information about antithreat technology.
More Symantec solutions	Takes you to the Symantec Store Web site, from which you can get product information on every Symantec product.

Within your Symantec product, the Reports page contains a link to the Symantec online Virus Encyclopedia, as does the Windows Explorer toolbar.

To access the Web site from the Reports page

- 1 In the main window, under Norton AntiVirus, click **Reports**.
- 2 On the Reports page, next to Online Virus Encyclopedia, click **View Report**.

To access the Symantec Web site from Windows Explorer

- 1 Open Windows Explorer.
- 2 On the toolbar, on the Norton AntiVirus menu, click **View Virus Encyclopedia**.
This option connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.

To access the Symantec Web site in your browser

- ❖ On the Internet, go to www.symantec.com

Subscribe to the Symantec Security Response newsletter

Each month, Symantec publishes a free electronic newsletter that is focused on the needs of Internet security customers. It discusses the latest antivirus technology produced by Symantec Security Response, common viruses, trends in virus workings, virus outbreak warnings, and special *virus definitions* releases.

To subscribe to the Symantec Security Response newsletter

- 1 On the Internet, go to securityresponse.symantec.com
- 2 On the security response Web page, scroll down to the reference area of the page, then click **Newsletter**.
- 3 On the security response newsletter Web page, select the language in which you want to receive the newsletter.
- 4 On the subscribe Web page, type the information requested, then click **Subscribe**.

The default settings for this product provide complete protection for your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply. You can change the product's settings to fit your work environment.

If you are using Windows 2000/XP, you will need administrator access to change options. If you are an administrator and share your computer with others, keep in mind that the changes that you make apply to everyone using the computer.

Set Norton Internet Security Professional options

The default settings for Norton Internet Security Professional provide a safe, automatic, and efficient way of protecting your computer. If you want to change or customize your protection, you can access all Norton Internet Security Professional tools from the Status & Settings window.



Restricted users cannot make changes to Norton Internet Security Professional settings. All users, regardless of their access levels, can make changes to Norton AntiVirus, UnErase, WipeInfo, and Web Tools settings. To protect your settings from unwanted changes, set a password for Norton Internet Security Professional and Norton AntiVirus options.

To change settings for individual features

- 1 In the main window, do one of the following:
 - Double-click a feature you want to customize.
 - Select a feature, then in the lower-right corner of the window, click **Customize**.
- 2 Configure the feature.
- 3 When you are done making changes, click **OK**.

If you have installed accounts, you can customize some Norton Internet Security Professional features for individual users. Other settings apply to all users.

To change settings for individual accounts

- 1 In the main window, do one of the following:
 - Double-click a feature you want to customize.
 - Select a feature, then in the lower-right corner of the window, click **Customize**.
- 2 In the feature's window, on the Settings For menu, select the account that you want to configure.

Set Norton Internet Security Professional options

- 3 Configure the feature.
- 4 When you are done making changes, click **OK**.



If you are using Windows 2000/XP and you do not have Local Administrator access, you cannot change Norton Internet Security Professional options.

To customize Norton Internet Security Professional

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton Internet Security**.
- 2 Select the tab on which you want to change options.
Your options are:

General	See "About General options" on page 93.
LiveUpdate	See "About LiveUpdate options" on page 93.
Firewall	See "About Firewall options" on page 94.
Email	See "About Email options" on page 94.

About General options

See ["Password protect Norton Internet Security Professional options"](#) on page 94.

General options let you control when Norton Internet Security Professional starts, protect program settings with a password, and choose visual elements you want to display.

About LiveUpdate options

See ["Keeping current with LiveUpdate"](#) on page 103.

LiveUpdate options let you enable and disable Automatic LiveUpdate, which automatically checks for updates when you are connected to the Internet. For maximum security, you should leave this option checked.

You can choose the components you want Automatic LiveUpdate to monitor. You can also choose whether Automatic LiveUpdate updates the components in the background or alerts you that there are updates available.

About Firewall options

Firewall options let you activate advanced protection features and customize the *ports* your computer uses to view Web pages. Most people will not need to make any changes to these settings.

About Email options

Email options let you control how Norton Internet Security Professional notifies you when it is scanning email messages for private information and spam.

Password protect Norton Internet Security Professional options

You can protect Norton Internet Security Professional options with a password. This lets you control who can make changes to your protection.

Each copy of Norton Internet Security Professional can have only one options password. If you have created accounts for multiple users, each user will share a single options password.

To protect security options with a password

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton Internet Security**.
- 2 On the General tab, check **Turn on Password Protection**.
- 3 In the Password and Confirm Password text boxes, type a password.
- 4 Click **OK**.

Reset options password

If you forget your options password, you can reset it.

To reset your security options password

- 1 Do one of the following:
 - On the Windows taskbar, click **Start > Settings > Control Panel**.
 - On the Windows XP taskbar, click **Start > Control Panel**.
- 2 In the Control Panel, double-click **Add/Remove Programs**.
- 3 In the list of currently installed programs, click **Norton Internet Security Professional**.
- 4 Do one of the following:
 - In Windows 2000/Me, click **Change/Remove**.
 - In Windows 98, click **Add/Remove**.
 - In Windows XP, click **Change**.
- 5 In the Remove Application window, click **Reset Password**.
- 6 In the password reset dialog box, in the Reset Password Key text box, type the Reset Password Key that appears above the text box.
The Reset Password Key is case-sensitive.
- 7 In the New Password and Confirm New Password text boxes, type a new password.
- 8 Click **OK**.
- 9 In the Remove Application window, click **Cancel**.
- 10 In the Exit? alert, click **Yes**.

Customize Norton AntiVirus

The default settings for Norton AntiVirus provide complete virus protection for your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply.

Norton AntiVirus provides password protection for your option settings. You can enable, change, and reset a password so that unauthorized users cannot tamper with your settings.

All of the options are organized into three main categories. The options contained under each category are as follows.

Category	Options
System	Auto-Protect Manual Scan
Internet	Email Instant Messenger LiveUpdate
Other	Threat Categories Inoculation (Windows 98/98SE/Me) Miscellaneous

This section does not describe how to change the individual options, but gives a general description of what they do and how you can find them. For specific information about a particular option, check the online Help.

About System options

The System options control scanning and monitoring of your computer. You use System options to determine what gets scanned, what the scan is looking for, and what

happens when a virus or virus-like activity is encountered.

With higher levels of protection, there can be a slight trade-off in computer performance. If you notice a difference in your computer's performance after installation, you may want to set protection to a lower level or disable those options that you do not need.

The System options that you can set are as follows.

Option	Description
Auto-Protect	<p>Determine if Auto-Protect starts when you start your computer, what it looks for while monitoring your computer, and what to do when a virus is found.</p> <p>Auto-Protect options also include Bloodhound, Advanced, and Exclusions subcategories.</p> <ul style="list-style-type: none">■ Bloodhound is the scanning technology that protects against unknown viruses. Use these options to set its level of sensitivity in Auto-Protect.■ Advanced options determine the activities to be monitored when scanning for virus-like activities and when scanning floppy disks.■ Exclusions specify the files that should not be scanned by file name extension or by specific file name. Be careful not to exclude the types of files that are more likely to be infected by viruses such as files with macros or executable files.
Manual Scan	<p>Determine what gets scanned and what happens if a virus or threat is found during a scan that you request.</p> <p>Manual Scan options also include Bloodhound and Exclusions subcategories.</p>

About Internet options

Internet options define what happens when your computer is connected to the Internet. You use Internet options to define how Norton AntiVirus should scan email and instant messenger attachments, enable Worm Blocking, and determine how updates should be applied with LiveUpdate.

The Internet options you can set are as follows.

Option	Description
Email	Enable email scanning and Worm Blocking, and define how Norton AntiVirus should behave while scanning email messages. Scanning incoming email messages protects your computer against viruses sent by others. Scanning outgoing email messages prevents you from inadvertently transmitting viruses or worms to others. You can choose to scan incoming or outgoing email messages, or both, and to display an icon or progress indicator while scanning. You can set options to automatically repair, quarantine, or delete infected email messages with or without interaction with you. Advanced options determine what to do when scanning email messages.
Instant Messenger	Determine what instant messengers to support, how to configure a new instant messenger, and what happens if a virus is found during an instant messenger session.
LiveUpdate	Enable Automatic LiveUpdate and define how updates should be applied. Automatic LiveUpdate checks for updated virus definitions automatically when you are connected to the Internet.

About Other options

Other options include Inoculation settings for Windows 98/98SE/Me and Miscellaneous settings. You can enable Inoculation, cause an alert if a system file changes, set a variety of miscellaneous options, and customize behavior for the Norton Protected Recycle Bin.

The Other options that you can set are as follows.

Option	Description
Threat Categories	Determine the threats that you want Norton AntiVirus to detect. Advanced options include how to respond when a threat is found and what to do when deleting threats. Exclusions options specify the files that should not be scanned by file name extension or by specific file name.
Inoculation	Enable Inoculation and, if a system file changes, choose to update the Inoculation snapshot or repair the file by restoring it to its original values. Inoculation options are available only on Windows 98/98SE/Me.
Miscellaneous	Back up file in Quarantine before attempting a repair. (This option is automatically set to On.) Enable Office Plug-in. If you upgrade to Microsoft Office 2000 or later after Norton AntiVirus is installed, you must enable this option to automatically scan Microsoft Office files. Alert me if my virus protection is out of date. Scan files at system startup (Windows 98/98SE only). Enable password protection for options.

Set Norton AntiVirus options

You change the settings for Norton AntiVirus options in the Options window.



If you set a password for Options, Norton AntiVirus asks you for the password before you can continue.

To change settings

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, in the left pane, select an option in the list.
Options with an arrow to the left have sub-options. As you select an option, the corresponding settings for the selected option appear in the right pane.
- 3 Select any settings that you want to change.
- 4 Click **OK**.
These settings now take precedence over the preset options. The changes take effect immediately.

If you need to restore default Norton AntiVirus settings

You can change any or all of the options listed. If you have made a number of changes that have unwanted results, you can restore all options to the default settings.



If you set a password for Options, Norton AntiVirus asks you for the password before you can view or adjust the settings.

To restore default settings on an Options page

- ❖ On the page for which you want to restore default settings, click **Page Defaults**.

To restore default settings for all options

- ❖ On any page in the Options window, click **Default All**.

Password protect Norton AntiVirus options

To protect your Norton AntiVirus options from being changed without your permission, you can choose to protect or remove protection from your option settings with a password. If you specify a password, you are asked to enter a password every time that you view the Options window, or temporarily enable or disable Auto-Protect.

If you forget your password, you can reset it from the Help button in the Norton AntiVirus main window. See the online Help for more information about resetting your password.

To specify or remove a password

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under Other, click **Miscellaneous**.
- 3 Check or uncheck **Enable password protection for options**.
- 4 In the password dialog box, type a password.
- 5 Click **OK**.

Set Wipe Info options

You can specify how Wipe Info handles files with *hidden*, read-only, and system attributes. You can also specify the type of wipe to use. The following wiping methods are available.

Fast Wipe	Overwrites the data that is being wiped with the hexadecimal value of your choice
Government Wipe	Combines several wiping and overwriting processes to conform to specifications in DoD (Department of Defense) document 5220-22-M, National Industrial Security Program Operating Manual, for the ultimate security level when eliminating data from digital media See "About the Government Wipe process" on page 194.

To change Wipe Info options

- 1 In the Security Center, click **Norton AntiVirus > Advanced Tools**.
- 2 On the Wipe Info line, click **Start Tool**.
- 3 Click **Options**.
- 4 On the General tab, select the options for Read-only, System, and Hidden file types.
- 5 On the Wipe Type tab, select the type of wipe that you want to perform. Your options are:
 - Fast Wipe
 - Government Wipe
- 6 In the Hex Value text box, type the hexadecimal values that Wipe Info should use when it overwrites the wiped files space.
- 7 In the Times to Perform This Wipe text box, type the number of times that Wipe Info should repeat this process.
- 8 Click **Apply**.

See ["About hexadecimal values"](#) on page 194.

Keeping current with LiveUpdate

6

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate obtains program updates and protection updates for your computer.

Your normal Internet access fees apply when you use LiveUpdate.



If your computer uses Windows 2000/XP, you must have Administrator *access privileges* to run LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of obtaining and installing program updates. It locates and obtains files from an Internet site, installs them, and then deletes the leftover files from your computer.

About protection updates

Protection updates are files that are available from Symantec that keep your Symantec products up-to-date with the latest anti-threat technology. The protection updates you receive depend on which product you are using.

Norton AntiVirus, Norton AntiVirus Professional, Norton SystemWorks, Norton SystemWorks Professional, Symantec AntiVirus for Handhelds – Annual Service Edition	Users of Norton AntiVirus, Norton SystemWorks, and Symantec AntiVirus for Handhelds – Annual Service Edition products receive virus protection updates, which provide access to the latest virus signatures and other technology from Symantec.
Norton Internet Security, Norton Internet Security Professional	<p>In addition to the virus protection updates, users of Norton Internet Security products also receive protection updates for Web filtering, intrusion detection, and Norton AntiSpam.</p> <p>The Web filtering protection updates provide the latest lists of Web site addresses and Web site categories that are used to identify inappropriate Web content.</p> <p>The intrusion detection updates provide the latest predefined firewall rules and updated lists of applications that access the Internet. These lists are used to identify unauthorized access attempts to your computer.</p> <p>Norton AntiSpam updates provide the latest spam definitions and updated lists of spam email characteristics. These lists are used to identify unsolicited email.</p>
Norton Personal Firewall	Users of Norton Personal Firewall receive intrusion detection updates for the latest predefined firewall rules and updated lists of applications that access the Internet.
Norton AntiSpam	Users of Norton AntiSpam receive the latest spam definitions and updated lists of spam email characteristics.

Obtain updates using LiveUpdate

LiveUpdate checks for updates to all of the Symantec products that are installed on your computer.



If your *Internet service provider* does not automatically connect you to the Internet, connect to the Internet first, and then run LiveUpdate.

To obtain updates using LiveUpdate

- 1 At the top of the main window, click **LiveUpdate**.
- 2 In the LiveUpdate window, click **Next** to locate updates.
- 3 If updates are available, click **Next** to download and install them.
- 4 When the installation is complete, click **Finish**.



Some program updates may require that you restart your computer after you install them.

When you should update

Run LiveUpdate as soon as you have installed your product. Once you know that your files are up-to-date, run LiveUpdate regularly to obtain updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

If you can't use LiveUpdate

When new updates become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can obtain new updates from the Symantec Web site.

To obtain updates from the Symantec Web site

- 1 On the Internet, go to securityresponse.symantec.com
- 2 Follow the links to obtain the type of update that you need.

Set LiveUpdate to Interactive or Express mode

LiveUpdate runs in either Interactive or Express mode. In Interactive mode (the default), LiveUpdate *downloads* a list of updates that are available for your Symantec products that are supported by LiveUpdate technology. You can then choose which updates you want to install. In Express mode, LiveUpdate automatically installs all available updates for your Symantec products.

To set LiveUpdate to Interactive or Express mode

- 1 At the top of the main window, click **LiveUpdate**.
- 2 In the LiveUpdate welcome screen, click **Configure**.
- 3 In the LiveUpdate Configuration dialog box, on the General tab, select the mode that you want. Your options are:

Interactive Mode	Gives you the option of choosing which updates you want to install
Express Mode	Automatically installs all available updates

- 4 If you selected Express Mode, select how you want to start checking for updates. Your options are:

I want to press the start button to run LiveUpdate	Gives you the option of cancelling the update
I want LiveUpdate to start automatically	Installs updates automatically whenever you start LiveUpdate

- 5 To have access to a Symantec self-help Web site in the event that an error occurs while using LiveUpdate, check **Enable Enhanced Error Support**.
- 6 Click **OK**.

Turn off Express mode

Once you have set LiveUpdate to run in Express mode, you can no longer access the LiveUpdate Configuration dialog box directly from LiveUpdate. You must use the Symantec LiveUpdate control panel.

To turn off Express mode

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 In the Control Panel window, double-click **Symantec LiveUpdate**.
- 3 In the LiveUpdate Configuration dialog box, on the General tab, click **Interactive Mode**.
- 4 Click **OK**.

If you run LiveUpdate on an internal network

If you run LiveUpdate on a computer that is connected to a network that is behind a company firewall, your network administrator might set up an internal LiveUpdate server on the network. LiveUpdate should find this location automatically.

If you have trouble connecting to an internal LiveUpdate server, contact your network administrator.

Run LiveUpdate automatically

You can have LiveUpdate check for protection updates automatically, on a set schedule, by enabling Automatic LiveUpdate. You must continue to run LiveUpdate manually to receive product updates.



Automatic LiveUpdate checks for an Internet connection every five minutes until a connection is found, and then every four hours. If you have an ISDN router that is set to automatically connect to your Internet service provider (ISP), many connections will be made, with connection and phone charges possibly being incurred for each connection. If this is a problem, you can set your ISDN router to not automatically connect to the ISP or disable Automatic LiveUpdate.

To enable Automatic LiveUpdate

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton Internet Security**.
If you set a password for Options, you must provide the password before you can continue.
- 2 In the Options dialog box, on the LiveUpdate tab, check **Enable Automatic LiveUpdate**.
- 3 If you want to be notified when updates are available, check **Notify me when Norton Internet Security Professional updates are available**.
- 4 Select the updates for which you want Automatic LiveUpdate to check.

- 5 For each type of update for which you want Automatic LiveUpdate to check, select how you want those updates to be applied. Your options are:

Automatically update my protection	LiveUpdate checks for and installs protection updates without prompting you. LiveUpdate displays an alert when a protection update has been downloaded. You should still run LiveUpdate occasionally to check for program updates.
Notify me	LiveUpdate checks for protection updates and asks if you want to install them.

- 6 Click **OK**.

To delete the schedule for Automatic LiveUpdate, disable Automatic LiveUpdate.

To disable Automatic LiveUpdate

- 1 At the top of the main window, click **Options**.
 If a menu appears, click **Norton Internet Security**.
 If you set a password for Options, you must provide the password before you can continue.
- 2 In the Options dialog box, on the LiveUpdate tab, uncheck **Enable Automatic LiveUpdate**.
- 3 Click **OK**.

About your subscription

See ["About protection updates"](#) on page 104.

Your Symantec product includes a complimentary, limited-time subscription to protection updates that are used by your product. When the subscription is due to expire, you are prompted to renew your subscription.

If you do not renew your subscription, you can still use LiveUpdate to obtain program updates. However, you cannot obtain protection updates through LiveUpdate or from the Symantec Web site and will not be protected against newly discovered [threats](#). Also, whenever you use LiveUpdate, you will receive a warning that your subscription has expired. Follow the on-screen instructions to complete your subscription renewal.

Guarding against intrusion attempts

7

The Personal Firewall and Intrusion Detection features protect your computer from online attacks, unwanted connection attempts, malicious Web content, port scans, and other suspicious behavior.

About the Personal Firewall

When the Personal Firewall is active, it monitors communications among your computer and other computers on the Internet. It also protects your computer from such common security problems as the following.

Improper connection attempts	Warns you of any connection attempts from other computers and attempts by programs on your computer to connect to other computers
Security and privacy incursions by malicious Web content	Monitors all Java applets and ActiveX controls and lets you choose whether to run or block the program
Port scans	Cloaks inactive ports on your computer and detects port scans
Intrusions	Detects and blocks malicious traffic and attempts by outside users to attack your computer

See ["Customize firewall protection"](#) on page 112.

You can control the level of protection that the Personal Firewall provides by using the Security Level slider. You can also control how the Personal Firewall reacts to

improper connection attempts, Trojan horses, and malicious Web content.

Customize firewall protection

The default Personal Firewall settings should provide adequate protection for most users. If the default protection is not appropriate, you can customize Personal Firewall protection by using the Security Level slider to select preset security levels, or by changing individual security settings.

Change the Security Level

The Security Level slider lets you select Minimal, Medium, or High security settings. When you change the slider position, the protection level changes. Changing the Security Level does not affect the protection provided by Intrusion Detection.

See "About Norton Internet Security Professional accounts" on page 156.

You can set individual Security Level settings for each Norton Internet Security Professional user.

To change the Security Level

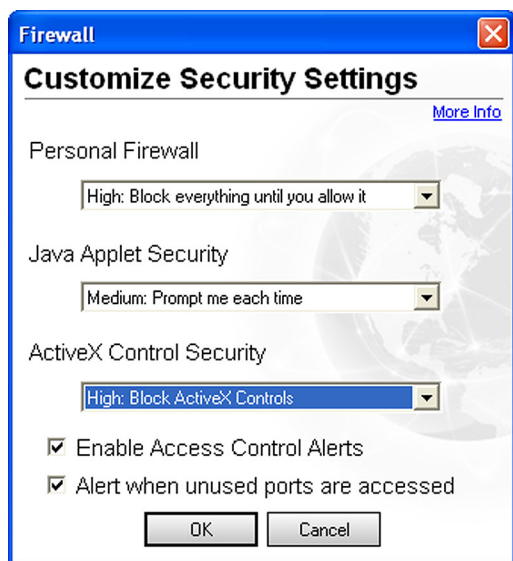
- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, in the Choose a security level for drop-down list, select the account that you want to change.
- 3 Move the slider to the Security Level that you want. Click **OK**.

Change individual security settings

If the Security Level options do not meet your needs, you can change the settings for the Personal Firewall, *Java*, and *ActiveX* protection levels. Changing an individual setting overrides the Security Level, but it does not change the other security settings in that level.

To change individual security settings

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, in the Choose a security level for drop-down list, select the account that you want to change.
- 3 Click **Custom Level**.



- 4 Do one or more of the following:
 - In the Personal Firewall drop-down list, select a level.
 - In the Java Applet Security or ActiveX Control Security drop-down list, select a level.
 - To be notified whenever unknown programs access the Internet, check **Enable Access Control Alerts**.
 - To be notified whenever a remote computer attempts to connect to a port no program is using, check **Alert when unused ports are accessed**.
- 5 Click **OK**.

Allow or block access to your computer

Norton Internet Security Professional allows you to organize computers on your local network and the Internet into Trusted and Restricted Zones. Zones allow you to grant trusted computers more access to your computer while blocking malicious users.

Computers in the Trusted Zone are not regulated by the Personal Firewall. They have as much access to your computer as they would have if you did not have a firewall. Computers in the Restricted Zone cannot communicate with your computer at all.

The Workgroup Network Wizard is the fastest way to organize computers into zones. You can also manually add individual computers to zones.

To categorize computers with the Workgroup Network Wizard

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Networking tab, click **Wizard**.
- 3 In the Workgroup Network Wizard opening window, click **Next**.
- 4 In the resulting list, check the network adapters that you want to configure automatically and add to your Trusted Zone.
- 5 Click **Next**.
- 6 Click **Finish** to close the wizard.

To manually add computers to zones

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Networking tab, select the zone to which you want to add a computer.
- 3 If you have turned on Network Detector, select the Location you want to customize.
- 4 Click **Add**.

See “Identify computers to Norton Internet Security Professional” on page 121.

- 5 In the Specify Computers window, identify the computer.
- 6 When you have finished adding computers, click **OK**.

To remove computers from zones

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Networking tab, select the zone containing the computer you want to remove.
- 3 If you have turned on Network Detector, select the Location you want to customize.
- 4 Select the computer that you want to remove.
- 5 Click **Remove**.
- 6 When you have finished removing computers, click **OK**.

Customize firewall rules

Firewall rules control how the Personal Firewall protects your computer from malicious incoming traffic, programs, and *Trojan horses*. The firewall automatically checks all data coming in or out of your computer against these rules.

How firewall rules are processed

Firewall rules are processed in a set order based on their types. System rules are processed first, followed by program rules, and then Trojan horse rules.

Once a rule that blocks or permits communications is matched, all remaining rules are ignored. In other words, additional rules that match this type of communication are ignored if they appear below the first rule that matches.

If no matching rule is found, the communication is blocked.

Create new firewall rules

See “About Norton Internet Security Professional accounts” on page 156.

Program Control, helps you create firewall rules as you use the Internet.

If you are administering multiple computers, you can create firewall rules on your computer and then transfer them to the other computers. This gives you more control over your organization’s protection, but may cause problems if a Restricted user needs to use a program that you do not have installed on your computer. Supervisor and Standard users can create and modify firewall rules while using the program, but Restricted users cannot make any changes to firewall rules.

There are four ways to create firewall rules with Program Control:

Enable Automatic Program Control	Automatically configures access for well-known programs the first time that users run them. This is the easiest way to set up firewall rules.
Use Program Scan	Finds and configures access for all Internet-enabled programs on a computer at once.
Manually add programs	Closely manage the list of programs that can access the Internet.
Respond to alerts	Norton Internet Security Professional warns users when a program attempts to access the Internet for the first time. Users can then allow or block Internet access for the program.

Enable Automatic Program Control

Automatic Program Control automatically configures Internet access settings for programs the first time that they run. Automatic Program Control only configures Internet access for the versions of programs that Symantec has identified as safe.

When Automatic Program Control configures access for a new program, Norton Internet Security Professional displays a message above the Windows toolbar.

If an unknown program or an unknown version of a known program attempts to access the Internet, you receive an alert. You can then choose to allow or block Internet access for the program.

To enable Automatic Program Control

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Programs tab, select the Location you want to customize.
- 3 Check **Turn on Automatic Program Control**.
- 4 Click **OK**.

Scan for Internet-enabled programs

Scanning for Internet-enabled programs lets you quickly customize Internet access for multiple programs. Program Scan scans the computer for programs that it recognizes and suggests appropriate settings for each program.

To scan for Internet-enabled programs

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Programs tab, click **Program Scan**.
- 3 Select the disk or disks on your computer that you want to scan.
- 4 Click **Next**.
- 5 In the Program Scan window, review the list of Internet-enabled programs that Program Scan identified.
- 6 Do one of the following:
 - Check the boxes next to the programs you want to configure.
 - To customize the Internet access settings Program Scan suggested for a program, select it, then click **Modify**.
 - To leave a program unconfigured, uncheck the box next to the program. You will receive an alert the next time this program accesses the Internet.
- 7 Click **Next**.

- 8 If you have turned on Network Detector, select the Locations that should use these settings.
- 9 Click **Finish**.
- 10 Click **OK**.

Manually add a program to Program Control

See “Customize firewall protection” on page 112.

Add programs to Program Control to strictly control the programs’ ability to access the Internet. This overrides any settings made by Automatic Program Control.

To add a program to Program Control

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Programs tab, select the Location you want to customize.
- 3 Click **Add**.
- 4 Select the program’s executable file. Executable file names typically end in .exe.
- 5 Click **Open**.
- 6 In the Program Control alert, select the access level you want this program to have.
- 7 To see risks that this program could pose to your computer, click **Show Details**.
- 8 Click **OK**.

Customize Program Control

After using Norton Internet Security Professional for a while, you may find that you need to change access settings for certain programs.

To customize Program Control

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Programs tab, select the Location you want to customize.
- 3 In the list of programs, click the program that you want to change.
- 4 Click **Modify**.

- 5 In the Program Control alert, select the access level you want this program to have.
- 6 Click **OK**.

Manually add a firewall rule

While Program Control automatically creates most of the firewall rules that you need, you may want to add specific rules. Only experienced Internet users should create their own firewall rules.

There are three sets of firewall rules you can customize:

- General Rules
- Trojan Horse Rules
- Program Rules

To add a General Rule

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Advanced tab, click **General**.
- 3 Follow the on-screen instructions.

To add a Trojan Horse Rule

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Advanced tab, click **Trojan Horse**.
- 3 Follow the on-screen instructions.

To add a Program Rule

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Programs tab, in the list of programs, click **Add**.
- 3 In the Select a program window, select a program's executable file.
Executable file names typically end in .exe.
- 4 In the Program Control alert, on the What do you want to do menu, click **Manually configure Internet access**.
- 5 Follow the on-screen instructions.

Change an existing firewall rule

You can change firewall rules if they are not functioning the way that you want.

To change an existing firewall rule

- 1 In the General Rules, Trojan Horse Rules, or Program Rules window, select the rule that you want to change.
If you have turned on Network Detector, select the Location that should use the modified rule.
- 2 Click **Modify**.
- 3 Follow the on-screen instructions to change any aspect of the rule.
- 4 When you have finished changing rules, click **OK**.

Change the order of firewall rules

See “How firewall rules are processed” on page 115.

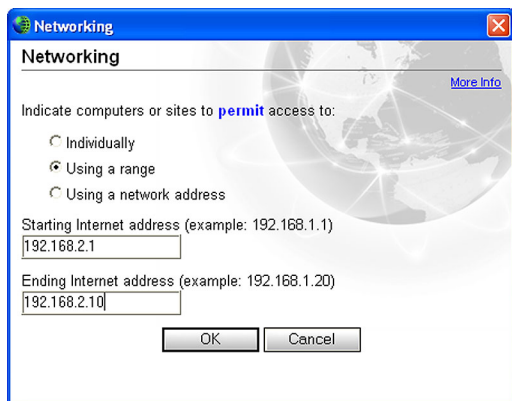
Each list of firewall rules is processed from the top down. You can adjust how firewall rules are processed by changing their order.

To change the order of a firewall rule

- 1 In the General Rules, Trojan Horse Rules, or Program Rules window, select the rule that you want to move.
If you have turned on Network Detector, select the Location that should use the modified rule.
- 2 Do one of the following:
 - To process this rule before the rule above it, click **Move Up**.
 - To process this rule after the rule below it, click **Move Down**.
- 3 When you are done moving rules, click **OK**.

Identify computers to Norton Internet Security Professional

You must identify computers to Norton Internet Security Professional to manually configure zones and firewall rules. In these cases, a dialog box appears to help you identify the computer.



There are three ways to identify computers. Each uses *IP addresses*.

Specify an individual computer

The computer name that you type can be an IP address, a URL such as `service.symantec.com`, or a Microsoft Network computer name, such as Mojave. You can find the names of computers on your local network in Network Neighborhood or Network Places on your Windows desktop.

To specify an individual computer

- 1 In the dialog box, click **Individually**.
- 2 Type the name or IP address of a single computer.
- 3 Click **OK**.

Specify a range of computers

You can enter a range of computers by specifying the starting (lowest numerically) IP address and the ending (highest numerically) IP address. All of the computers within that range of IP addresses are included.

In almost every case, the first three of the four numbers of the IP addresses entered should be the same.

To specify a range of computers

- 1 In the dialog box, click **Using a range**.
- 2 In the Starting Internet Address text box, type the starting (lowest numerically) IP address.
- 3 In the Ending Internet Address text box, type the ending (highest numerically) IP address.
- 4 Click **OK**.

Specify computers using a network address

You can identify all of the computers on a single [subnet](#) by specifying an IP address and a subnet mask. The IP address that you specify can be any address in the subnet that you are identifying.

To specify computers using a network address

- 1 In the dialog box, click **Using a network address**.
- 2 In the Network Address text box, type the IP address of a computer on the subnet.
- 3 In the Subnet Mask text box, type the subnet mask. The appropriate subnet mask is almost always 255.255.255.0.
- 4 Click **OK**.

About Intrusion Detection

Intrusion Detection scans all the network traffic that enters and exits your computer and compares this information against a set of attack signatures, arrangements of information that identify an attacker's attempt to exploit a known operating system or program vulnerability.

If the information matches an attack signature, Intrusion Detection automatically discards the packet and severs the connection with the computer that sent the data. This protects your computer from being affected in any way.

Intrusion Detection protects your computer against most common Internet attacks, including the following.

Bonk	An attack on the Microsoft TCP/IP stack that can crash the attacked computer
RDS_Shell	A method of exploiting the Remote Data Services component of the Microsoft Data Access Components that lets a remote attacker run commands with system privileges
WinNuke	An exploit that can use NetBIOS to crash older Windows computers

Intrusion Detection does not scan for intrusions by computers in your Trusted Zone. However, Intrusion Detection does monitor the information that you send to Trusted computers for signs of zombies and other remote control attacks.

See ["Keeping current with LiveUpdate"](#) on page 103.

Intrusion Detection relies on an extensive list of attack signatures to detect and block suspicious network activity. Run LiveUpdate regularly to ensure that your list of attack signatures is up to date.

Customize Intrusion Detection

The default Intrusion Detection settings should provide adequate protection for most users. You can customize Intrusion Detection by excluding specific network activity from monitoring, enabling or disabling AutoBlock, and restricting blocked computers.

Turn Intrusion Detection alerts on and off

See ["Identify the source of Internet traffic"](#) on page 63.

You can choose whether you want to receive alerts when Intrusion Detection blocks suspected attacks. The alerts include more information about the attacking computer and information about the attack. You can also trace the connection attempt using Visual Tracking.

To turn Intrusion Detection alerts on and off

- 1 In the main window, double-click **Intrusion Detection**.



- 2 In the Intrusion Detection window, check or uncheck **Notify me when Intrusion Detection blocks connections**.
- 3 Click **OK**.

Exclude specific network activity from being monitored

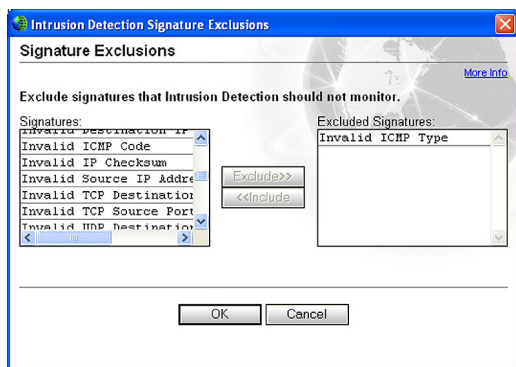
In some cases, benign network activity may appear similar to an attack signature. If you receive repeated warnings about possible attacks, and you know that these warnings are being triggered by safe behavior, you can create an exclusion for the attack signature that matches the benign activity.



Each exclusion that you create leaves your computer vulnerable to attacks. Be very selective when excluding attacks. Only exclude behavior that is always benign.

To exclude attack signatures from being monitored

- 1 In the main window, double-click **Intrusion Detection**.
- 2 In the Intrusion Detection window, click **Advanced**.



- 3 In the Signatures list, select the attack signature that you want to exclude.
- 4 Click **Exclude**.

- 5 When you are done excluding signatures, click **OK**.
- 6 In the Intrusion Detection window, click **OK**.

If you have excluded attack signatures that you want to monitor again, you can include them in the list of active signatures.

To include attack signatures

- 1 In the main window, double-click **Intrusion Detection**.
- 2 In the Intrusion Detection window, click **Advanced**.
- 3 In the Excluded Signatures list, select the attack signature that you want to monitor.
- 4 Click **Include**.
- 5 When you are done including signatures, click **OK**.
- 6 In the Intrusion Detection window, click **OK**.

Enable or disable AutoBlock

When Norton Internet Security Professional detects an attack, it automatically blocks the connection to ensure that your computer is safe. The program can also activate AutoBlock, which automatically blocks all incoming communication from the attacking computer for a set period of time, even if the incoming communication does not match an attack signature.

If AutoBlock is blocking a computer or computers you need to access, you can turn off AutoBlock. Make sure to turn AutoBlock back on when you are done.

To turn AutoBlock on and off

- 1 In the main window, double-click **Intrusion Detection**.
- 2 In the Intrusion Detection window, check or uncheck **Turn on AutoBlock**.
- 3 Click **OK**.

By default, AutoBlock blocks each computer for 30 minutes. Use the drop-down menu to choose how long you want to block attacking computers.

To customize the AutoBlock duration

- 1 In the main window, double-click **Intrusion Detection**.
- 2 In the Intrusion Detection window, under AutoBlock, on the AutoBlock attacking computer for menu, select a new duration.
- 3 Click **OK**.

See “[Stop all Internet communication](#)” on page 64.

AutoBlock stops all inbound communications with a specific computer. To stop all inbound and outbound communication with all computers, use Block Traffic.

Unblock AutoBlocked computers

If a computer that you need to access appears on the list of computers currently blocked by AutoBlock, unblock it. If you have changed your protection settings and want to reset your AutoBlock list, you can unblock all of the computers on the AutoBlock list at once.

To unblock computers currently blocked by AutoBlock

- 1 In the main window, double-click **Intrusion Detection**.
- 2 In the Intrusion Detection window, do one of the following:
 - To unblock one computer, select its IP address, then click **Unblock**.
 - To unblock all computers on the AutoBlock list, click **Unblock All**.
- 3 Click **OK**.

Exclude computers from AutoBlock

If a computer you need to access is repeatedly placed in the AutoBlock list, you can exclude it from being blocked by AutoBlock.

To exclude specific computers from AutoBlock

- 1 In the main window, double-click **Intrusion Detection**.
- 2 In the Intrusion Detection window, click **Exceptions**.

- 3 Do one of the following:
 - In the Currently blocked list, select a blocked IP address, then click **Exclude**.
 - Click **Add**, then type the computer's name, IP address, network identification, or a range of IP addresses containing the computer that you want to exclude.
- 4 When you are done excluding IP addresses, click **OK**.
- 5 In the Intrusion Detection window, click **OK**.

Restrict a blocked computer

You can add a blocked computer to your Restricted Zone to permanently prevent that computer from accessing your computer. Computers in the Restricted Zone do not appear on the blocked list because all communication with restricted computers is blocked.

To restrict a blocked computer

- 1 In the main window, double-click **Intrusion Detection**.
- 2 In the list of computers that are currently blocked by AutoBlock, select the computer to add to the Restricted Zone.
- 3 Click **Restrict**.
- 4 When you are done restricting computers, click **OK**.
- 5 In the Intrusion Detection window, click **OK**.

Customizing protection for different locations

8

Use Network Detector to create and customize security settings for different networks. This makes it easy for mobile users who connect to the Internet from the road to stay protected at all times.

About Network Detector

Network Detector lets you customize Program Control and Trusted Zone settings for different locations. A location is a group of security settings that can contain one or more networks. Whenever your computer connects to a network in one of these locations, Norton Internet Security Professional automatically switches to the security settings that are associated with that location.

For example, if you use your laptop to connect to the Internet from home, from work, and from a neighborhood coffeehouse, you are actually connecting to at least three different networks. If you want the same level of security in both your home and office, you could place both networks in a single location. If you want more security in the coffeehouse, you can create a high-security location for that network.

Norton Internet Security Professional includes four preconfigured locations.

Office	Low security. Primarily for use on networks containing a hardware firewall.
Home	Medium security. Good for general use.
Away	High security. Primarily for use on public networks.
Default	Security level is based on your current settings.

Create a new location

You can also create new locations with customized settings and names. For example, you could create a low-security Hotels location you use while traveling and a high-security Coffeehouse location for wireless networks provided by many coffeehouses.

If you regularly switch between several networks, you may find that this gives you more control over your protection.

You can create a new location from a Network Detector alert and from the main Norton Internet Security Professional window.

To create a new location from a Network Detector alert

- 1 In the Network Detector alert, on the Which location do you want to use menu, select **Use custom settings**.
- 2 In the Use Custom Settings window, click **Create new location**.
- 3 Click **Next**.
- 4 In the Setup Program Control window, do one of the following:

- Click **Yes (recommended)** to turn on Automatic Program Control.
This reduces the number of alerts that you receive.
- Click **No** to turn off Automatic Program Control.
You will be alerted the first time that programs attempt to connect to the Internet.

- 5 Click **Next**.
- 6 In the Save location window, type a name for this new location.
Choose a unique name so that this location is easy to identify.
- 7 Click **Next**.
- 8 In the Save location window, review this location's settings.
- 9 Click **Finish**.

To create a new location from the main window

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Locations tab, click **Wizard**.
- 3 In the Setup Program Control window, do one of the following:
 - Click **Yes (recommended)** to turn on Automatic Program Control.
This reduces the number of alerts that you receive.
 - Click **No** to turn off Automatic Program Control.
You will be alerted the first time that programs attempt to connect to the Internet.
- 4 Click **Next**.
- 5 In the Save location window, type a name for this new location.
Choose a unique name so that this location is easy to identify.
- 6 Click **Next**.
- 7 In the Save location window, review this location's settings.
- 8 Click **Finish**.

Add new networks to locations

Network Detector alerts you every time that your computer connects to an unrecognized network. You can choose to place this network in an existing location or create a new location.

To add a new network to one of the preconfigured locations

- ❖ In the Network Detector alert, on the Which location do you want to use menu, select a location.

To create a new location for this network

- 1 In the Network Detector alert, on the Which location do you want to use menu, click **Use custom settings**.
- 2 Use the Network Detector Wizard to create a new location.

See ["Create a new location"](#) on page 130.

To add a new network to a custom location that you have created

- 1 In the Network Detector alert, on the Which location do you want to use menu, click **Use custom settings**.
- 2 In the Use custom settings window, on the Choose a location drop-down menu, select the location that you want to use.
- 3 Click **Finish**.

Learn more about networks

Network Detector alerts include detailed information about networks that your computer joins. The details section of a Network Detector alert includes information about the following.

Gateway MAC id	The Media Access Control (MAC) address of this network's router
Gateway IP address	The IP address of this network's router
Subnet identifier	The subnet mask used on this network
Interface type	How your computer is connected to this network

Interface connection description	Information about the network adapter that made the connection
Domain	This network's domain name (if available)

To learn more about networks

- ❖ In the Network Detector alert, click **Show details**.

Customize a location's settings

You can customize the Program Control and Trusted Zone settings for the predefined locations and any new locations that you create. Any changes that you make will apply to all of the networks that use the location.

To customize a location's settings

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, do one of the following:
 - To change Automatic Program Control settings, click the **Programs** tab.
 - To change Trusted Zone settings, click the **Networking** tab.
- 3 In the Settings for menu, select the location you want to customize.
- 4 When you are finished making changes, click **OK**.

Remove networks from a location

If you've added a network to a location, you will not be alerted the next time your computer joins that network. If you want to change a network's security settings, you must clear the location that contains it. The next time that you use a network that had been in this location, Network Detector will ask you to choose a new location.

To clear networks from a location

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Location tab, in the list of locations, select the location that you want to clear.
- 3 Click **Clear**.
- 4 When you are finished clearing networks, click **OK**.

Delete a location

If you no longer need a location, or if you want to reassign the networks in a location, delete the location. The next time that you use a network that had been in this location, Network Detector will ask you to choose a new location.



You cannot delete the preconfigured Home, Office, Away, or Default locations.

To delete a location

- 1 In the main window, double-click **Personal Firewall**.
- 2 In the Personal Firewall window, on the Locations tab, in the list of locations, select the location that you want to delete.
- 3 Click **Delete**.
- 4 When you are finished deleting locations, click **OK**.

Protecting disks, files, and data from viruses

9

Keeping your computer protected requires regular monitoring by Auto-Protect and Worm Blocking; scanning of your email attachments and files transferred by instant messenger; and frequent system scans. All of these tasks can be set to occur automatically.

For added protection in Norton AntiVirus on Windows 98/98SE/Me, enable Inoculation to alert you if a system file changes.

Ensure that protection settings are enabled

Norton AntiVirus is configured to provide you with complete protection against viruses. It is unlikely that you need to change any settings. However, for maximum protection, you should ensure that your protection features are enabled.



For specific information about a particular option and its protection settings, see the online Help.

This table summarizes the maximum protection settings and where you can find them.

Feature	In the main window, click	Then for maximum protection, select
Auto-Protect	Norton AntiVirus > Auto-Protect > Enable	On

Feature	In the main window, click	Then for maximum protection, select
Email scanning	Options > Norton AntiVirus > Email	<ul style="list-style-type: none"> ■ Scan incoming Email ■ Scan outgoing Email <p>If your email program uses one of the supported communications protocols, both options are selected by default.</p>
Timeout protection	Options > Norton AntiVirus > Email	<p>Protect against timeouts when scanning Email</p> <p>To prevent connection timeouts while receiving large attachments, enable timeout protection.</p>
Instant messenger scanning	Options > Norton AntiVirus > Instant Messenger	Instant messengers that you want to protect
Worm Blocking	Options > Norton AntiVirus > Email	<ul style="list-style-type: none"> ■ Enable Worm Blocking ■ Alert me when scanning email attachments
Inoculation (Windows 98)	Options > Norton AntiVirus > Inoculation	Inoculate Boot Records

Manually scan disks, folders, and files

If Auto-Protect is enabled and the Norton AntiVirus options are set at their default levels, you normally would not need to scan manually. However, if you temporarily disabled Auto-Protect (for example, to load or use another program that conflicts with Norton AntiVirus), and you forgot to enable it again, it is possible that a virus could be on your hard disk undetected. You can scan your entire computer, or individual floppy disks, drives, folders, or files.

Although the default settings for manual scanning are usually adequate, you can raise the level of Bloodhound heuristics or adjust the options for manual scanning in the Options window.

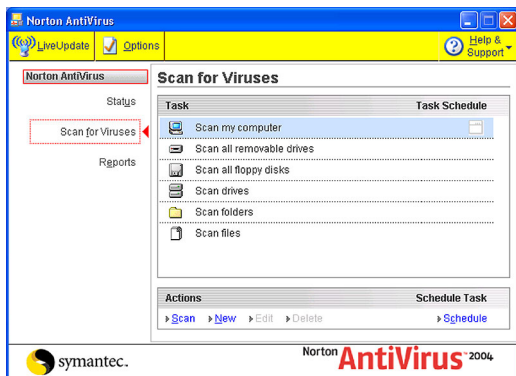
For more information about manual scanning options, see the online Help.

Perform a full system scan

A full system scan scans all *boot records* and files on your computer.

To perform a full system scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.



- 2 In the Scan for Viruses pane, under Task, click **Scan my computer**.
- 3 Under Actions, click **Scan**.
When the scan is complete, a scan summary appears.
- 4 When you are done reviewing the summary, click **Finished**.

Scan individual elements

Occasionally, you may want to scan a particular file, removable drives, a floppy disk, any of your computer's drives, or any folders or files on your computer. You may have been working with floppy disks or have received a compressed file in an email message and suspect a virus. You can scan just a particular disk or individual element that you want to check.

To scan individual elements

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the scan that you want to run.
- 3 Under Actions, click **Scan**.
If you choose to scan all removable drives or a floppy disk, the scan starts automatically. If you choose to scan drives, folders, or files, a dialog box appears in which you choose which drives, folders, or files to scan.
- 4 In the dialog box, make your selection, then click **Scan**.
When the scan is complete, a scan summary appears.
- 5 When you are done reviewing the summary, click **Finished**.

If problems are found during a scan

See ["What to do if a virus is found"](#) on page 145.

At the end of a scan, a summary report appears to tell you what Norton AntiVirus found during the scan. If a virus was found and you have requested that Norton AntiVirus repair the file automatically, it is listed as repaired. If the file cannot be repaired, it can be quarantined or deleted.

Create and use custom scans

See ["Schedule a custom scan"](#) on page 141.

You can create a custom scan if you regularly scan a particular segment of your computer and don't want to have to specify the segment to be scanned every time. You can also schedule the custom scan to run automatically.

You can delete the scan when it is no longer necessary. For example, if you are working on a project for which you need to frequently swap files with others, you might want to create a folder into which you copy and scan those files before using them. When the project is done, you can delete the custom scan for that folder.

To create a custom scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Actions, click **New**.
- 3 In the opening window of the Norton AntiVirus Scan Wizard, click **Next**.
- 4 Select the items that you want to scan. Your options are:

Add files	Select individual files to be scanned.
Add folders	Select folders and drives to be scanned.

You can use both options to select the combination of items that you want.

- 5 In the resulting dialog box, select the items that you want to scan.
If you select a folder, all files in that folder are included. If you select a drive, all folders and files on that drive are included.
- 6 Add the selected items to the list of items to scan by doing one of the following:
 - In the Scan Files dialog box, click **Open**.
 - In the Scan Folders dialog box, click **Add**.

- 7 If you need to remove an item from the list, select it, then click **Remove**.
- 8 When you are done creating the list of items to be scanned, click **Next**.
- 9 Type a name for the scan by which you can identify it in the list of scans.
- 10 Click **Finish**.

Run a custom scan

When you run a custom scan, you do not have to redefine what you want to scan.

To run a custom scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the custom scan.
- 3 Under Actions, click **Scan**.
When the scan is complete, a scan summary appears.
- 4 When you are done reviewing the summary, click **Finished**.

Delete a custom scan

You can delete custom scans if they are no longer needed.

To delete a custom scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the custom scan that you want to delete.



If you click the button next to the scan name, the scan runs.

- 3 Under Actions, click **Delete**.
- 4 Click **Yes** to verify that you want to delete the scan.

Schedule scans

After installation, Norton AntiVirus automatically runs a weekly full system scan. You can also set up a schedule for custom virus scans.

You can schedule customized virus scans that run unattended on specific dates and times or at periodic intervals. If you are using the computer when the scheduled scan begins, it runs in the background so that you do not have to stop working.



You cannot schedule the predefined scans in the scan list, but you can schedule any custom scans that you have created.

Schedule a custom scan

You have complete flexibility in scheduling custom scans. When you select how frequently you want a scan to run (such as daily, weekly, or monthly), you are presented with additional fields with which you can refine your request. For example, you can request a daily scan, then schedule it to occur every two days or every three days instead.

To schedule a custom scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the custom scan that you want to schedule.



- If you click the button next to the scan name, the scan runs.
- 3 Under Schedule Task, click **Schedule**.
 - 4 In the Schedule dialog box, if Show multiple schedules is checked, click **New** to enable the scheduling fields.
If it is not checked, the fields are already enabled.
 - 5 Set the frequency and time at which you want the scan to run.
Most of the frequency options include additional

options that let you further refine the schedule. Set the additional options as necessary.

- 6 When you are done, click **OK**.

You can also create multiple schedules for a scan. For example, you could run the same scan at the beginning of your work day and at the end.

To create multiple schedules for a single scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the custom scan that you want to schedule.



If you click the button next to the scan name, the scan runs.

- 3 Under Schedule Task, click **Schedule**.
- 4 In the Schedule dialog box, check **Show multiple schedules**.
- 5 To set an additional schedule, click **New**.
- 6 Set the frequency and time at which you want the scan to run.
Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.
- 7 When you are done, click **OK**.

Edit scheduled scans

You can change the schedule of any scheduled scan, including the weekly full system scan.

To edit a scheduled scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the scan that you want to reschedule.



If you click the button next to the scan name, the scan runs.

- 3 Under Schedule Task, click **Schedule**.

- 4 Change the schedule as desired.
- 5 Click **OK**.

Delete a scan schedule

You can delete any scan schedule. Deleting the schedule does not delete the scan.

To delete a scan schedule

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the scan whose schedule you want to delete.



If you click the button next to the scan name, the scan runs.

- 3 Under Schedule Task, click **Schedule**.
- 4 In the Schedule dialog box, check **Show multiple schedules**.
- 5 Select the schedule or schedules that you want to delete.
- 6 Click **Delete**.
- 7 Click **OK**.



What to do if a virus is found

10



If after reviewing the information in this chapter, you have not resolved your problem, see [“Responding to emergencies”](#) on page 17 and [“Troubleshooting”](#) on page 217.

If Norton AntiVirus finds a virus or a file containing a virus or a potential security risk on your computer, there are several possible resolutions to the problem:

- **Fix infection**
Removes the virus from the file or if the threat is a worm or Trojan horse, deletes the file.
- **Quarantine infection**
Makes the file inaccessible by any programs other than a Symantec antivirus program. You cannot accidentally open the file and spread the virus, but you can still evaluate it for possible submission to Symantec.
- **Delete the file**
Removes the virus from your computer by deleting the file that contains the virus, worm, or Trojan horse. It should be used only if the file cannot be repaired or quarantined.
- **Exclude at-risk files**
Excludes the files at risk from future scans. If you exclude a file, you are doing so permanently from future scans. The threat may still be on your computer.

See [“If Norton AntiVirus places files in Quarantine”](#) on page 152.

Viruses can be found during a manual or scheduled scan or by Auto-Protect when you perform an action with an

infected file. Threats and security risks can appear during an instant messenger session, when sending an email message, or during a manual or scheduled scan.

If a virus is found during a scan

If Norton AntiVirus finds a virus, Trojan horse, worm, or security risk during a scan or from an instant messenger session, you either receive a summary of the automatic repair or deletion results, or use the Repair Wizard to resolve the problem.

Review the repair details

If you have set your manual scan options so that Norton AntiVirus repairs or deletes files automatically, and all infected files could be repaired or deleted, the scan summary lists the number of files found, infected, and repaired or deleted. This information is presented for status purposes only; you don't need to take further action to protect your computer. If you want to know more, you can check the repair details to see which files were infected and with which [threats](#).

To review the repair details

- 1 In the scanner window, in the Summary pane, click **More Details**.
- 2 When you are done reviewing the results, click **Finished**.

Use the Repair Wizard

If there are files that could not be fixed, or if you have set options so that Norton AntiVirus asks you what to do when a virus or threat is found, the Repair Wizard opens. If Norton AntiVirus did not attempt a repair, the Repair Wizard opens in the Fix Infection pane. Otherwise, it opens in the Quarantine window.

To use the Repair Wizard

- 1 If the Repair Wizard opens in the Fix Infections pane, uncheck any files that you don't want Norton AntiVirus to fix.

All files are checked by default. This is the recommended action.

- 2 Click **Fix**.

If any files cannot be fixed or deleted, the Quarantine Infections window opens. All files are checked to be added to Quarantine by default. This is the recommended action.

- 3 In the Quarantine window, uncheck any files that you do not want to quarantine.

- 4 Click **Quarantine**.

If any files could not be quarantined, the Delete window opens. All files are checked to be deleted by default.

- 5 In the Delete window, uncheck any files that you do not want to delete.



If you do not delete the infected files, the virus or file at risk remains on your computer and can cause damage or be transmitted to others.

- 6 Click **Delete**.

If any files could not be deleted, the Exclude At-risk Files window opens to allow you to exclude files considered to be at risk from future scans.

- 7 In the Exclude At-risk Files window, select any files that you want to exclude.

- 8 Click **Exclude**.

- 9 Once all of the files have been repaired, quarantined, deleted, or excluded, the Scan Summary window opens.



If any files could not be deleted, they appear in the Scan Summary window with a status of at risk or delete failed. There are a variety of reasons why some files cannot be deleted: a file could be in use or part of a larger program. Norton AntiVirus recommends that you select the threat name to review the information

from the Internet and determine the appropriate action.

- 10 When you are done reviewing the summary, click **Finished**.

If a virus is found by Auto-Protect

See ["Ensure that protection settings are enabled"](#) on page 135.

Auto-Protect scans files for viruses when you perform an action with them, such as moving them, copying them, or opening them. If it detects a virus or virus-like activity, in most cases you receive an [alert](#) telling you that a virus was found and repaired. How you proceed depends on the operating system that you are using.

If you are using Windows 98/98SE/Me

If a virus or threat is found and repaired by Auto-Protect in Windows 98/98SE/Me, you receive an [alert](#) telling you which file was repaired or deleted.

To close the alert

- ❖ Click **Finish**.

If you have set your options so that Auto-Protect asks you what to do when it finds a virus, the alert asks you to choose one of the following actions. The recommended action is always preselected.

Action	Result
Repair the infected file	Automatically eliminates the virus, Trojan horse, or worm and repairs or deletes the infected file. When a virus is found, Repair is always the best choice.
Quarantine the infected file	Isolates the infected file, but does not remove the threat. Select Quarantine if you suspect that the infection is caused by an unknown threat and you want to submit the threat to Symantec for analysis.

Action	Result
Delete the infected file	Erases both the threat and the infected file. Select Delete if Repair is not successful. Replace the deleted file with the original program file or backup copy. If the virus, Trojan horse, or worm is detected again, your original copy is infected.
Do not open the file, but leave the problem alone	Stops the current operation to prevent you from using an infected file. This action does not solve the problem. You will receive an alert the next time that you perform the same activity.
Ignore the problem and do not scan this file in the future	Adds the file that is suspected of containing a threat to the Exclusions list. When you add a file to the Exclusions list, the file is excluded from any future virus scans, unless you remove it from the list. Select this option only if you know that the file does not contain a virus.
Ignore the problem and continue with the infected file	Continues the current operation. Select this option only if you are sure that a virus, Trojan horse, or worm is not at work. You will receive an alert again. If you are not sure what to do, select Do not open the file, but leave the problem alone.

If a file cannot be repaired, you receive an alert telling you that the repair was not made and recommending that you quarantine the file. You have the same options as those listed in the table, with the exception of Repair the infected file.

If you are using Windows 2000/XP

If a virus is found and either repaired or automatically deleted by Auto-Protect in Windows 2000/XP, you receive an *alert* telling you which file was repaired or deleted and which virus, Trojan horse, or worm was infecting the file. If you have an active Internet connection, selecting the virus name opens the Symantec Web page that describes the virus.

If Auto-Protect finds a virus in a compressed file, such as a .zip file, the alert displays the name and location of the compressed file. To stop further alerts for viruses found

in this compressed file, select the option “Don’t alert me about this file again.”

To close the alert

❖ Click **OK**.

If the file cannot be repaired, you receive two alerts, one telling you that Auto-Protect was unable to repair the file, and another telling you that access to the file was denied.

You can set your Auto-Protect options to try to quarantine any infected files that it cannot repair. If you do this, you are informed if any files are quarantined.

To resolve problems with unrepaired files

- 1 Run a full system scan on your computer to ensure that no other files are infected.
- 2 Follow the recommended actions in the Repair Wizard to protect your computer from the infected files.

See “If Norton AntiVirus places files in Quarantine” on page 152.

See “If a virus is found during a scan” on page 146.

If a threat is found by Worm Blocking

See “Ensure that protection settings are enabled” on page 135.

If a program tries to email itself or email a copy of itself, it could be a worm trying to spread via email. A *worm* can send itself or a copy of itself in an email message without any interaction with you.

Worm Blocking continually scans outgoing email attachments for worms. If it detects a worm, you receive an *alert* telling you that a malicious worm was found.

The alert presents you with options and asks you what to do. If you were not sending an email message at that time, then it is probably a worm and you should quarantine the file. You can click Help on the alert for additional information about how to respond.

After you have responded to the *threat* and deleted the file, you could still have an infected system. Follow these procedures.

Procedure	For more information
Run LiveUpdate to ensure that you have the latest protection updates.	See " About protection updates " on page 104.
Scan your system.	See " Perform a full system scan " on page 137.
Go to the Symantec Security Response Web page for the most up-to-date virus definitions and clean-up tools.	See the Symantec Security Response Web page at securityresponse.symantec.com

If Inoculation alerts you about a change in system files



See "[Ensure that protection settings are enabled](#)" on page 135.

Inoculation protection is available on Windows 98/98SE/Me systems only.

System files can change for a variety of reasons. You may have updated your operating system or repartitioned your hard disk, or you could have a virus. Norton AntiVirus alerts you when a change occurs in your system files.

If you get an *alert* about a change in your system files, you have two options. You can update your Inoculation snapshot or repair the file. Before you repair the file, be sure that your virus definitions are up-to-date and run a scan.

To respond to Inoculation changes

- ❖ In the Alert window, select the action that you want to take. Your options are:

Update the saved copy of my Master Boot Record	Use if the alert appears after a legitimate change in system files.
Restore my Master Boot Record	Use if you are certain the system did not change for legitimate reasons.

If Norton AntiVirus places files in Quarantine

Once a file has been placed in Quarantine, you have several options. All of the actions that you take on files in Quarantine must be performed in the Quarantine window.

The toolbar at the top of the Quarantine window contains all of the actions that you can perform on quarantined files.

Add Item	Adds files to Quarantine. Use this action to quarantine a file that you suspect is infected. This action has no effect on files that are already in Quarantine.
Properties	Provides detailed information about the selected file and the virus that is infecting it.
Repair Item	Attempts to repair the selected file. Use this action if you have received new virus definitions since the file was added to Quarantine.
Restore Item	Returns the selected file to its original location without repairing it.
Delete Item	Deletes the selected file from your computer.

Submit Item	Sends the selected file to Symantec. Use this option if you suspect that a file is infected even if Norton AntiVirus did not detect it.
LiveUpdate	Runs LiveUpdate to check for new protection and program updates. Use this if you haven't updated your virus definitions for a while and then try to repair the files in Quarantine.

To open the Quarantine window

- 1 On the left side of the main window, under Norton AntiVirus, click **Reports**.
- 2 In the Reports pane, on the Quarantined items line, click **View Report**.

To perform an action on a file in Quarantine

- 1 In the Quarantine window, select the file on which you want to perform the action.
- 2 On the toolbar, select the action that you want to perform.
- 3 When you are finished, on the File menu, click **Exit**.

If Norton AntiVirus cannot repair a file

See ["Keeping current with LiveUpdate"](#) on page 103.

One of the most common reasons that Norton AntiVirus cannot automatically repair or delete an infected file is that you do not have the most up-to-date virus definitions. Update your virus definitions with LiveUpdate and scan again.

If that does not work, read the information in the report window to identify the types of items that cannot be

Look up viruses on the Symantec Web site

repaired, and then take one of the following actions, depending on the file type.

File type	Action
Infected files with .exe, .doc, .dot, or .xls file name extensions (any file can be infected)	Use the Repair Wizard to solve the problem. For more information, see the online Help.
Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files	Replace using the Rescue Disks or your operating system disks. For more information, see the online Help.

Look up viruses on the Symantec Web site

The Symantec Web site contains a complete list of all known viruses and related malicious code, along with descriptions. You must be connected to the Internet to look up viruses.

To look up viruses

- 1 On the left side of the main window, under Norton AntiVirus, click **Reports**.
- 2 In the Reports pane, on the Online Virus Encyclopedia line, click **View Report**.
The Symantec Web site opens in your Internet browser.
- 3 Use the links on the Web page to access the virus information for which you are looking.

Creating accounts for multiple users

11

If you are responsible for managing several computers, you can use Norton Internet Security Professional to simplify administering security settings. Norton Internet Security Professional lets network administrators create customized security settings for individual users. You can also export settings files that can be used to establish standard protection for all computers in an office.

Norton Internet Security Professional uses accounts to control access to the Internet. An account stores the type of Internet access that is allowed for the users assigned to the account. If several people share a computer, you can create accounts that are specific to the needs of each user.

About Norton Internet Security Professional accounts

Your computer can host several accounts, but all accounts fall within one of the following three access levels.

Restricted	Cannot make any changes to Norton Internet Security Professional protection. Has limited access to Internet programs and Web site categories.
Standard	Can customize all Norton Internet Security Professional options for own account.
Supervisor	Can change all Norton Internet Security Professional options for all users.

There is also a default account, Not Logged In, that blocks all Internet access. When a user logs off, the settings for Not Logged In become active and stay active until another user logs on.

See ["Set or change account passwords"](#) on page 161.

When you install Norton Internet Security Professional, the program creates a default account with Supervisor privileges. This account is not password-protected. For maximum security, you should create a password for this account.

Norton Internet Security Professional accounts and Windows accounts

See ["Assign Norton Internet Security Professional account types to Windows accounts"](#) on page 162.

You can choose to create Norton Internet Security Professional accounts or Windows accounts. The primary difference between the two types of accounts is that the Windows accounts are tied to the operating system. If you log in to Windows using a Windows account, you will also be logged in to Norton Internet Security Professional with that account.

Manage accounts on multiple computers

The User Access Manager lets you create and manage accounts for multiple users on multiple computers. You can either manually configure each computer or create settings for all of the users in your office on your computer. You can then export these settings to the other computers in your office.

After importing your settings, Supervisor and Standard users will be able to make changes to their protection. For maximum security, create Restricted users, then import the settings that you have customized. Restricted user cannot make changes to Norton Internet Security Professional settings.



The User Access Manager settings file does not include users' passwords. You should encourage users to choose passwords immediately after importing settings.

Create Norton Internet Security Professional accounts

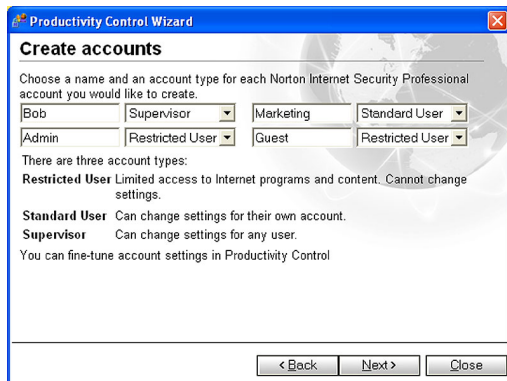
Supervisor users can create new accounts and customize settings for other users. They can also create new user accounts with the Security Assistant. Standard users can customize their own accounts, but cannot change other users' accounts. Restricted users can change their passwords only.

You can create several accounts at once with the Productivity Control Wizard or one-by-one using the User Accounts screen.

To create Norton Internet Security Professional accounts with the Productivity Control Wizard

- 1 In the main window, click **User Accounts**.
- 2 In the User Accounts window do one of the following:
 - If you are creating accounts for the first time, click **Yes** to run the Productivity Control Wizard.
 - If you have existing accounts, click **Productivity Control Wizard**.

- 3 In the Choose account manager screen, click **Create Norton Internet Security Professional accounts**.
- 4 Click **Next**.



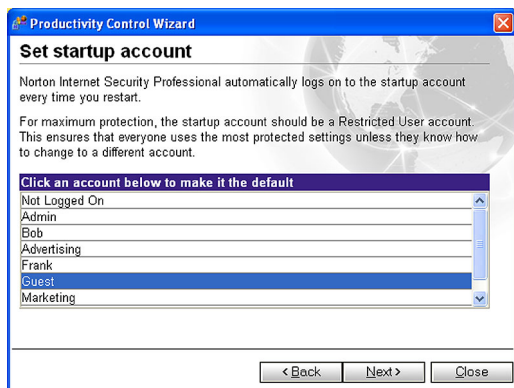
The screenshot shows a window titled "Productivity Control Wizard" with a close button in the top right corner. The main heading is "Create accounts". Below it, a text box says: "Choose a name and an account type for each Norton Internet Security Professional account you would like to create." There are two rows of input fields. The first row has "Bob" in a text box, a "Supervisor" dropdown menu, "Marketing" in a text box, and a "Standard User" dropdown menu. The second row has "Admin" in a text box, a "Restricted User" dropdown menu, "Guest" in a text box, and a "Restricted User" dropdown menu. Below these fields, a text box says: "There are three account types:". This is followed by three entries: "Restricted User" with the description "Limited access to Internet programs and content. Cannot change settings.", "Standard User" with "Can change settings for their own account.", and "Supervisor" with "Can change settings for any user.". A final line says: "You can fine-tune account settings in Productivity Control". At the bottom right, there are three buttons: "< Back", "Next >", and "Close".

- 5 In the Create accounts screen, type one or more account names.
- 6 On the account level menus, select an appropriate account level for each account.
- 7 Click **Next**.
- 8 In the Choose passwords screen, in the Password and Confirm Password text boxes, type a password for this user.

See ["Set or change account passwords"](#) on page 161.

9 Click **Next**.

If you have created more than one account, repeat the previous two steps with each account.



See ["Set the startup account"](#) on page 161.

10 In the Set startup account screen, select the account that Norton Internet Security Professional automatically logs on to when you restart the computer.

11 Click **Next**.

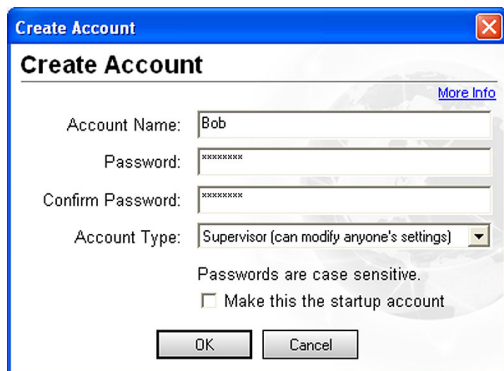
12 Click **Finish**.

To create Norton Internet Security Professional accounts with the User Accounts screen

- 1 In the main window, click **User Accounts**.



- 2 In the User Accounts screen, click **Create Account**.



- 3 In the Create Account dialog box, in the Account Name text box, type a name for this account.
- 4 In the Password and Confirm Password text boxes, type a password for this account. Passwords are case-sensitive.

- 5 On the Account Type menu, select an account type.
- 6 Click **OK**.

Set the startup account

Every time that you start your computer, Norton Internet Security Professional automatically logs on to the account that is designated as the startup account. To ensure that users do not make unwanted changes to Norton Internet Security Professional settings, you should create a Restricted account and set it as the default startup account.

To set an account as the startup account

- 1 In the main window, click **User Accounts**.
- 2 In the User Accounts screen, select the user account that you want to make the startup account.
- 3 Click **Properties**.
- 4 In the Account Properties dialog box, check **Make this the startup account**.
- 5 Click **OK**.

Set or change account passwords

For maximum security, you should protect each account with a password. This ensures that only approved users can access the Internet and your network.

To set or change your own password

- 1 In the main window, click **User Accounts**.
- 2 In the User Accounts screen, select your account.
- 3 Click **Change Password**.
- 4 In the Change Password dialog box, type your old password, then type your new password.
If the account did not previously have a password, the Old Password field is unavailable.
- 5 Click **OK**.

Standard users can change passwords for Restricted accounts. Supervisor users can change any other

Assign Norton Internet Security Professional account types to Windows accounts

accounts' passwords. If you change an account password, be sure to inform everyone who uses that account.

To set or change passwords for other users

- 1 In the main window, click **User Accounts**.
- 2 In the User Accounts screen, select the account that you want to change.
- 3 Click **Properties**.
- 4 In the Account Properties dialog box, in the Password and Confirm Password text boxes, type a new password.
- 5 Click **OK**.

Assign Norton Internet Security Professional account types to Windows accounts

If you have created Windows accounts for multiple users, you can use these accounts instead of creating new Norton Internet Security Professional accounts. Your Norton Internet Security Professional accounts use the same names as your Windows accounts.



If you plan to transfer your security settings to other users' computers, you must create Windows accounts for each user on your computer before configuring Norton Internet Security Professional.

To assign Norton Internet Security Professional account types to Windows accounts

- 1 In the main window, click **User Accounts**.
- 2 In the User Accounts window, do one of the following:
 - If you are creating accounts for the first time, click **Yes** to run the Productivity Control Wizard.
 - If you have existing accounts, click **Productivity Control Wizard**.
- 3 In the Choose account manager screen, click **Use existing Windows accounts**.

4 Click **Next**.

In the Choose account level screen, all of your currently defined Windows accounts are listed.



5 For each account, select an account type.

6 Click **Next**.

7 Click **Finish** to close the Productivity Control Wizard.

Log on to Norton Internet Security Professional

See ["About Norton Internet Security Professional accounts"](#) on page 156.

When you start Norton Internet Security Professional, it uses the settings from the account that you designated as the startup account.

To use a different account, you must log off of the current account and log on to another account. If you are not sure which account is active, you can check the active account.

To find out which account is active

- ❖ Open Norton Internet Security Professional.
 The active account is listed in the middle of the main window.

If you want to use a different account than the one that is currently active, you must log off of the current account, then log on with the account that you want to use.

To log on to another account

- 1 In the Windows system tray, right-click the Norton Internet Security Professional icon, then click **Log Off**.
- 2 Click **Yes** to confirm that you want to log off.
- 3 In the Windows system tray, right-click the Norton Internet Security Professional icon, then click **Account Login**.
- 4 In the Log On dialog box, select the account that you want to use.
- 5 Type the password, if required.
- 6 Click **OK**.

As soon as you change an account, Norton Internet Security Professional begins using the settings associated with that account. The Accounts window shows the account that is currently active.

Customize Norton Internet Security Professional accounts

Each Norton Internet Security Professional account can have personalized settings for the following features:

Feature	More information
Productivity Control	See "Controlling individuals' Internet use" on page 165.
Privacy Control	See "Protecting your privacy" on page 175.
Ad Blocking	See "Blocking Internet advertisements" on page 185.
Norton AntiSpam	See "Manage how Norton AntiSpam detects spam" on page 66.

Controlling individuals' Internet use

12

Productivity Control lets you manage individual users' Internet access by controlling the following:

Web sites	Block access to sexually explicit, violent, job search, or otherwise inappropriate Web pages.
Programs	Block categories of Internet programs that pose security risks or could be misused.
Newsgroups	Restrict access to discussion groups related to extreme, illegal, or inappropriate topics.



Restricted users cannot make any changes to Productivity Control settings.

About Productivity Control

When you enable Productivity Control, it blocks any incoming information from restricted Web sites and newsgroups. It also blocks all outgoing information from restricted Internet programs.

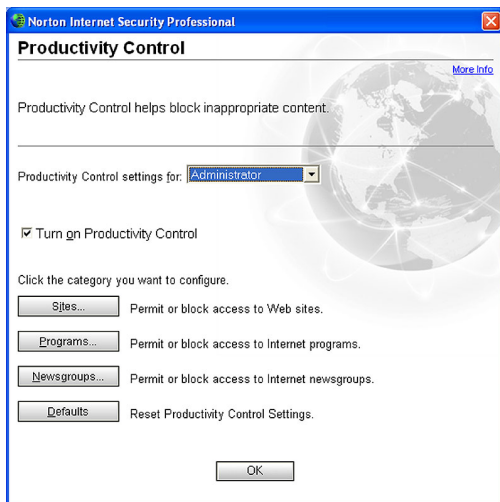
Productivity Control settings are linked to user accounts. When users log on to their accounts, Productivity Control uses the settings associated with the accounts until the users log off.

Enable or disable Productivity Control

Supervisor and Standard users can enable or disable Productivity Control. Standard users can change Productivity Control settings for their accounts. Supervisor users can also make changes to any user's Productivity Control settings. Restricted users cannot make any changes to Productivity Control.

To enable or disable Productivity Control

- 1 In the main window, double-click **Productivity Control**.



- 2 In the Productivity Control window, in the Productivity Control settings for drop-down list, select the account that you want to change.
- 3 Check or uncheck **Turn on Productivity Control**.

See "Review log information" on page 212.

Productivity Control tracks its activity on the Event Log's Restrictions tab. Check this tab periodically to monitor the effectiveness of your Productivity Control settings.

Customize Productivity Control

You can add or remove categories to or from the list of blocked Web sites, newsgroups, and Internet programs. You can also exclude specific sites and newsgroups from blocking and create a list of permitted Web sites and newsgroups.

Restrict Web site access

There are two ways to restrict Web site access:

- Block Web sites by category.
Specify which categories of sites users can and cannot access. You can also add or remove specific sites to or from the list of blocked sites in a category. Use this option to restrict users from visiting specific types of Web sites, but to allow everything else.
- Create a list of Web sites that can be visited.
Specify the Web sites that all users can visit. Use this option to strictly control users' Internet activities, as all Web sites not on the list are blocked, regardless of users' account types.

Block Web sites by category

Productivity Control includes an extensive list of categorized Web sites. You can select which categories of sites are appropriate for each account on your computer.

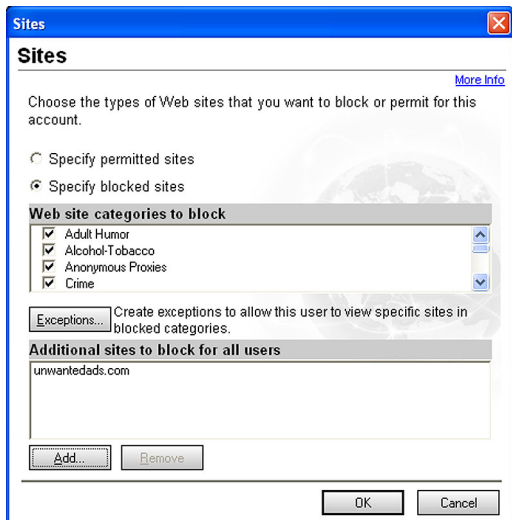
Before blocking Web sites by category, run LiveUpdate to ensure that the list of Web sites is up-to-date.

See "Keeping current with LiveUpdate" on page 103.

To block Web sites by category

- 1 In the main window, double-click **Productivity Control**.
- 2 In the Productivity Control window, in the Productivity Control settings for drop-down list, select the account that you want to change.

3 Click **Sites**.



- 4 In the Sites window, click **Specify blocked sites**.
- 5 Under Web site categories to block, check the categories that you want to block for this account.
- 6 Click **OK**.
- 7 When you are done specifying sites, click **OK**.

Block additional sites

Productivity Control lets you restrict access to specific Web sites or domains that are not included in one of the categories of blocked sites. If you block a domain, all Web sites within the domain are included. For example, if you block the domain `uninvitedads.com`, Productivity Control will block all Web sites at that domain, including `www.uninvitedads.com` and `images.uninvitedads.com`. If you block `images.uninvitedads.com`, only that Web site will be blocked.

To block or unblock specific sites

- 1 In the main window, double-click **Productivity Control**.
- 2 In the Productivity Control window, in the Productivity Control settings for drop-down list, select the account that you want to change.
- 3 Click **Sites**.
- 4 In the Sites window, click **Specify blocked sites**.
- 5 Click **Add**.
- 6 In the Add Web site to Blocked List window, type the URL of the site that you want to add.
- 7 Click **OK**.
- 8 Repeat the previous three steps for each Web site that you want to add.
- 9 When you are done adding sites, click **OK**.

Create exceptions for specific sites

If a site you need to view belongs to a blocked category, you can create an exception for this site. This allows you to permit access to specific Web sites that belong to blocked categories while still blocking other sites of this type.

To create exceptions for specific sites

- 1 In the main window, double-click **Productivity Control**.
- 2 In the Productivity Control window, in the Productivity Control settings for drop-down list, select the account that you want to change.
- 3 Click **Sites**.
- 4 In the Sites window, click **Specify blocked sites**.
- 5 Click **Exceptions**.
- 6 In the Exceptions window, click **Add**.
- 7 In the Add Web site to Exception List window, type the URL of the site that you want to add.
- 8 Click **OK**.

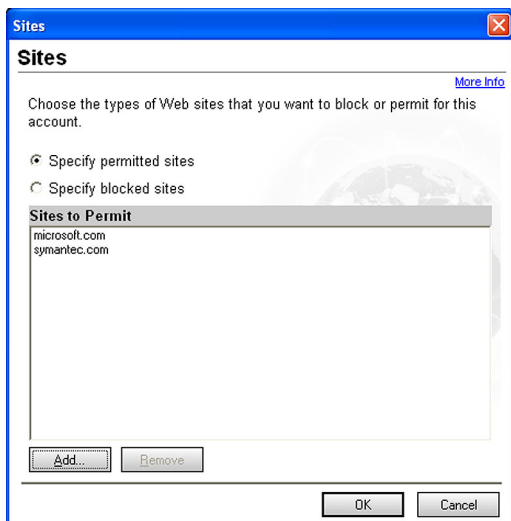
- 9 Repeat the previous three steps for each Web site that you want to add to your exceptions list.
- 10 When you are done adding sites, click **OK**.

Create a list of permitted Web sites

You can strictly control Web access by creating a list of Web sites that people using this computer are allowed to access. Any sites that are not on the list of permitted Web sites are blocked. Everyone who uses this computer can visit approved sites only, regardless of their account types.

To create a list of permitted Web sites

- 1 In the main window, double-click **Productivity Control**.
- 2 In the Productivity Control window, in the Productivity Control settings for drop-down list, select the account that you want to change.
- 3 Click **Sites**.



- 4 In the Sites window, click **Specify permitted sites**.

- 5 Click **Add** to create a new entry in the list.
- 6 In the Add Web site to Permitted List window, type the URL (Web address) of the site that you want to add.
- 7 Repeat the previous two steps for each Web site that you want to add.
- 8 Click **OK**.

Restrict programs that access the Internet

Programs access the Internet for many reasons. Your Web browser accesses the Internet to display Web pages. LiveUpdate accesses the Internet to retrieve program and protection updates for Symantec products. Microsoft NetMeeting accesses the Internet to let users conduct meetings over the Internet.

While most programs' Internet access attempts are benign, some *Trojan horses* and other programs may download malicious programming or upload personal information. Productivity Control lets you control how programs access the Internet. Productivity Control can block categories of Internet programs and limit how certain groups of Internet programs can be used.



Program limitations are intended for use with Restricted accounts. Users with Standard accounts will be able to override program restrictions on a per-program basis.

Block and permit categories of Internet programs

Productivity Control organizes Internet programs into categories. By default, Restricted users can access the Internet with programs in the General, Email, Web Browsers, and User categories only.

Blocking a program from accessing the Internet does not prevent users from running the program. A program may stop responding when Productivity Control prevents it from connecting to the Internet. Before making changes to program settings, ensure that users understand that their computers may stop responding if they use blocked programs.

To block and permit categories of Internet programs

- 1 In the main window, double-click **Productivity Control**.
- 2 In the Productivity Control window, on the Settings For menu, select the account that you want to change.
- 3 Click **Programs**.



- 4 In the Programs dialog box, under Program Categories, select the categories of programs that this account is allowed to use.
- 5 Click **OK**.

Restrict newsgroup access

Productivity Control blocks newsgroups based on text strings, which are groups of letters found in the names of the newsgroups.

When users access newsgroups, Productivity Control compares the names of the newsgroups that they attempt to view with a list of text strings you create. Productivity Control then blocks or permits access to newsgroups containing those text strings.

When newsgroups are blocked, newsreader programs will not include their names in the master list of available newsgroups that users can view. If a user attempts to

See "To block and permit categories of Internet programs" on page 172.

post a message in the newsgroup, Norton Internet Security Professional automatically blocks the post.

By default, Restricted users cannot use newsreader programs. To allow Restricted users to view newsgroups, you must unblock the newsreaders program category.

Enter text strings to block or permit



Productivity Control includes a list of text strings that block newsgroups that many people would find objectionable. You can add strings to customize Productivity Control.

Each computer can have only one list of permitted or blocked newsgroups.

To enter text strings to block or permit

- 1 In the main window, double-click **Productivity Control**.
- 2 In the Productivity Control window, on the Settings For menu, select the account that you want to change.
- 3 Click **Newsgroups**.
- 4 In the Specify Newsgroups window, select the action that you want to take. Your options are:

Specify permitted newsgroups	Identify text strings to permit.
Specify blocked newsgroups	Identify text strings to block.

- 5 Click **Add**.
- 6 Type a text string to block or permit.
- 7 Click **OK**.

Create exceptions to blocked newsgroups

If you create a list of blocked sites, you may find that a newsgroup that your users need to access is also blocked. Productivity Control lets you create exceptions that give

access to specific blocked newsgroups. For example, you can block access to all comp.security newsgroups while still allowing access to comp.security.firewalls.

To create exceptions to blocked newsgroups

- 1** In the main window, double-click **Productivity Control**.
- 2** In the Productivity Control window, on the Settings For menu, select the account that you want to change.
- 3** Click **Newsgroups**.
- 4** In the Specify Newsgroups window, click **Specify Blocked Newsgroups**.
- 5** Click **Exceptions**.
- 6** Click **Add**.
- 7** In the Add Newsgroup to Exceptions List window, type the complete name of the newsgroup that you want to unblock.
- 8** Click **OK**.
- 9** When you are done adding exceptions, click **OK**.

Every time that you browse the Internet, computers and Web sites collect information about you. Some of this information comes from forms that you fill out and choices that you make. Other information comes from your browser, which automatically provides information about the Web page you last visited and the type of computer that you're using.

Computers include some basic security features, but they might not be enough to protect your personal information. Privacy Control helps protect your privacy by giving you several levels of control over [cookies](#) and other information that your browser sends to Web sites.

Identify private information to protect

Many Web sites ask for your name, email address, and other personal information. While it is generally safe to provide this information to large, reputable sites, malicious sites can use this information to invade your privacy. It is also possible for people to intercept information sent via the Web, email, and instant messenger programs.

Privacy Control lets you create a list of information that you want to remain private. If users attempt to send protected information over the Internet, Privacy Control can warn them about the security risk or block the connection. All users on a protected computer share a single Private Information list.

Add private information

You must add information that you want to protect to the Private Information list. All users on a single computer share a single Private Information list.

To add private information

- 1 In the main window, double-click **Privacy Control**, then click **Private Information**.
- 2 In the Private Information dialog box, click **Add**.
- 3 In the Add Private Information dialog box, under Type Of Information To Protect, select a category.
- 4 In the Descriptive Name text box, type a description to help you remember why you are protecting this information.
- 5 In the Information To Protect text box, type the information that you want to block from being sent over insecure Internet connections.



Supervisor and Standard users can view information in the Private Information list. If you plan to transfer security settings to other computers, do not include personal information that you do not want to share with other people using this computer.

- 6 Under Secure this private information in, select the Internet programs in which Privacy Control should block this information. Your options are:
 - Web browsers
 - Instant messengers
 - Email programs
- 7 Click **OK**.

Modify or remove private information

You can modify or remove private information at any time.

To modify or remove private information

- 1 In the main window, double-click **Privacy Control**.
- 2 In the Privacy Control window, click **Private Information**.

- 3 Select the private information that you want to change or remove.
- 4 Select one of the following:
 - Modify
 - Remove
- 5 Click **OK**.

Customize Privacy Control

Privacy Control protects four areas:

Private Information	Blocks specific text that you do not want sent over the Internet
Cookie Blocking	Stops Web sites from retrieving personal information stored in cookie files
Browser Privacy	Protects information about your browsing habits
Secure Connections	Prevents users from establishing secure connections to online stores and other Web sites

Supervisor and Standard users can make changes to program settings. Restricted users cannot make any changes to Privacy Control.

There are two ways to adjust Privacy Control settings:

- **Set the Privacy Level.**
Use the slider in the main Privacy Control pane to select pre-set security levels.
- **Adjust individual Privacy Control settings.**
Customize your protection by manually adjusting individual settings.

You can set individual Privacy Control settings for each user.

Set the Privacy Level

Privacy Control offers pre-set security levels that help you set several options at one time. The Privacy Level slider lets you select minimal, medium, or high protection.

To set the Privacy Level

- 1 In the main window, double-click **Privacy Control**.
- 2 In the Privacy Control window, in the Privacy Control settings for drop-down list, select the account that you want to change.
- 3 Move the slider to the Privacy Level that you want.
- 4 Click **OK**.

Adjust individual Privacy Control settings

You can change the settings for Private Information, Cookie Blocking, Browser Privacy, and Secure Connections if the Privacy Level settings do not meet your needs. For example, you can choose to block all attempts to send private information while allowing Web sites to customize their pages using your browser information.

Change the Private Information setting

Change the Private Information setting to control how Privacy Control handles attempts to send information on the Private Information list over the Internet.

To change the Private Information setting

- 1 In the main window, double-click **Privacy Control**.
- 2 In the Privacy Control window, in the Privacy Control settings for drop-down list, select the account that you want to change.
- 3 Click **Custom Level**.
- 4 Select the Private Information setting that you want.
- 5 Click **OK**.

Change the Cookie Blocking setting

Many Web sites store information they collect in [cookies](#) placed on your hard disk. When you return to a site that has set a cookie on your computer, the Web server opens and reads the cookie.

Most cookies are harmless. Sites use them to personalize Web pages, remember choices that you have made on the site, and deliver optimized pages for your computer. However, sites can also use cookies to track your Internet usage and browsing habits.

Change the Cookie Blocking setting to control how Privacy Control handles sites that attempt to place cookies on your computer.

To change the Cookie Blocking setting

- 1 In the main window, double-click **Privacy Control**.
- 2 In the Privacy Control window, in the Privacy Control settings for drop-down list, select the account that you want to change.
- 3 Click **Custom Level**.
- 4 Select the Cookie Blocking setting that you want.
- 5 Click **OK**.

See ["Use Web assistant"](#) on page 62.

You can also customize cookie blocking for individual sites using Web assistant.

Enable or disable Browser Privacy

Browser Privacy prevents Web sites from learning the type of computer and browser that you are using, the Web site that you last visited, and other information about your browsing habits. Some Web sites that depend on JavaScript may not work correctly if they cannot identify the type of browser that you are using.

To enable or disable Browser Privacy

- 1 In the main window, double-click **Privacy Control**.
- 2 In the Privacy Control window, in the Privacy Control settings for drop-down list, select the account that you want to change.

- 3 Click **Custom Level**.
- 4 In the Customize Privacy Settings dialog box, check or uncheck **Enable Browser Privacy**.
- 5 Click **OK**.

Disable or enable secure Web connections

When you visit a secure Web site, your browser sets up an encrypted connection with the Web site. By default, all accounts can use secure connections. If you want to ensure that users are not sending private information to secure Web sites, you can disable secure Web connections.



If you disable secure Web connections, your browser will not encrypt any information that it sends. You should only disable secure Web connections if you are protecting your personal data in the Private Information list.

To disable or enable secure Web connections

- 1 In the main window, double-click **Privacy Control**.
- 2 In the Privacy Control window, in the Privacy Control settings for drop-down list, select the account that you want to change.
- 3 Click **Custom Level**.
- 4 In the Customize Privacy Settings dialog box, check or uncheck **Enable Secure Connections (https)**.
- 5 Click **OK**.

Blocking unwanted email messages

14

See [“Manage how Norton AntiSpam detects spam”](#) on page 66.

Norton AntiSpam uses a pattern-matching engine that automatically compares the contents of incoming email messages to a list of spam characteristics. If the message contains many spam characteristics, it is more likely to be spam than a message that contains few spam characteristics. Based on this analysis, Norton AntiSpam estimates the likelihood that the message is spam.

Norton AntiSpam uses the settings you’ve chosen to determine which messages are marked as spam. If Norton AntiSpam is set to Low, messages must contain many spam characteristics before they are flagged as spam. If Norton AntiSpam is set to High, messages that contain only a few spam characteristics are flagged.



Some email servers use [SSL \(Secure Sockets Layer\)](#) connections to encrypt connections between your computer and the server. Norton AntiSpam cannot scan email messages received via SSL connections.

Customize Norton AntiSpam

Customize your protection by identifying email addresses and particular text strings that should and should not be filtered. When Norton AntiSpam encounters a message containing one of these addresses or text strings, it immediately categorizes the message based on your settings. This helps ensure that messages from trusted senders do not get marked as spam.

Everyone using this computer shares a single customized Norton AntiSpam list. The User Access Manager settings file does not include Spam Blocking strings, so you will need to create your list on each computer.

Supervisor and Standard users can make changes to this list. Restricted users cannot make any changes to Norton AntiSpam settings.

To add a new Norton AntiSpam entry

- 1 In the main window, double-click **AntiSpam**.
- 2 In the Norton AntiSpam window, in the Norton AntiSpam settings for drop-down list, select the account that you want to change.
- 3 In the Norton AntiSpam window, click **Spam Rules**.
- 4 In the Spam Rules window, click **New**.
- 5 In the Search for text box, type an address or a text string.
- 6 Click **Next**.
- 7 Select where in incoming email messages Norton AntiSpam should search for the text. Your options are:
 - Entire email
 - From (sender's name)
 - Recipient
 - Subject line
 - Body text
- 8 Click **Next**.
- 9 Under Classify matching messages as, choose whether messages that include this text are spam or not spam.
- 10 Click **Next**.
- 11 Click **Finish**.
- 12 Click **OK** to close the Spam Rules window.

Modify or delete a Norton AntiSpam entry if it is causing messages to be incorrectly classified.

To modify or delete a Norton AntiSpam entry

- 1 In the main window, double-click **AntiSpam**.

- 2 In the Norton AntiSpam window, in the Norton AntiSpam settings for drop-down list, select the account that you want to change.
- 3 In the Norton AntiSpam window, click **Spam Rules**.
- 4 In the Spam Rules window, select the Norton AntiSpam entry with which you want to work.
- 5 Do one of the following:
 - Click **Edit** to change the entry, and follow the same steps as adding an entry.
 - Click **Delete** to delete the entry.
- 6 Click **OK** to close the Spam Rules window.

Change the priority of a spam rule

When Norton AntiSpam compares an email message to the list of spam rules, it starts with the rule at the top of the list, then continues down the list until it finds a match. When a match is found, Norton AntiSpam categorizes the email message accordingly and moves to the next message. If you find that the spam email messages you receive tend to match one rule more than the others, you may want to move that rule to the top of the list.

To change the priority of a spam rule

- 1 In the main window, double-click **AntiSpam**.
- 2 In the Norton AntiSpam window, click **Spam Rules**.
- 3 Select the rule that you want to move.
- 4 Do one of the following:
 - Click **Move Up** to make the rule a higher priority.
 - Click **Move Down** to make the rule a lower priority.
- 5 Click **OK**.



Blocking Internet advertisements

15

When Ad Blocking is enabled, it transparently removes:

- Ad banners
- Pop-up and pop-under ads
- Macromedia Flash-based ads

Use the Ad Trashcan

As you use the Internet, you may find ads that are not included on the default Ad Blocking list. You can use the Ad Trashcan to add these to your personal list of blocked ads.

To use the Ad Trashcan

- 1 Open your Web browser and view the page containing the advertisement that you want to block.
- 2 Open Norton Internet Security Professional.
- 3 In the main window, double-click **Ad Blocking**.
- 4 In the Ad Blocking window, ensure that Enable Ad Blocking is checked.
- 5 Click **Ad Trashcan**.
The Ad Trashcan window appears.
- 6 With the windows arranged so that you can see both the advertisement and the Ad Trashcan window, do one of the following:
 - If you are using Microsoft Internet Explorer, drag the unwanted ad from the Web site to the Ad Blocking dialog box.

- If you are using Netscape, right-click the advertisement, then click **Copy Image Location**. In the Ad Trashcan, click **Paste**. The address for the advertisement appears in the Ad Details line of the Ad Trashcan dialog box.
- 7 Select one of the following:
 - Add: Block this address.
 - Modify: Change the entry before adding it to the Ad Blocking list.
For example, if the advertisement address is <http://www.uninvitedads.org/annoying/ads/numberone.gif>, you could change it to <http://www.uninvitedads.org/annoying/ads/> to block everything in the ads directory.
 - 8 Click **Close**.
 - 9 Click **OK** to close the Ad Blocking window.

Use text strings to identify ads to block or permit

You can control whether Ad Blocking displays specific ads by creating a list of text strings that identify individual ad banners. Ad Blocking strings are sections of *HTML* addresses. If any part of a file's address matches the text string, Ad Blocking automatically blocks the file.

All users on a computer share a single Ad Blocking list. The User Access Manager settings file does not include custom Ad Blocking strings, so you will need to create your custom list on each computer.

Supervisor and Standard users can make changes to the list. Restricted users cannot make any changes to Ad Blocking settings.

How to identify Ad Blocking strings

The way that you define Ad Blocking strings affects how restrictive or unrestrictive Ad Blocking is when filtering data.

For example, if you add the string `uninvitedads.com` to the (Defaults) block list, you block everything in the `uninvitedads.com` domain. If you are more specific and add the string `nifty_images/image7.gif` to the site-specific block list maintained for `www.uninvitedads.com`, you block only that particular image.

Add an Ad Blocking string

You can add strings to the Ad Blocking list for all sites or for individual sites.

To add an Ad Blocking string

- 1 In the main window, double-click **Ad Blocking**.
- 2 In the Ad Blocking window, click **Advanced**.
- 3 On the left side of the Advanced window, do one of the following:
 - To block a string on all Web sites, click **(Defaults)**.
 - To block a string on a Web site in the list, select the site's name.
 - To block a string on a Web site not in the list, click **Add Site**, then in the New Site/Domain dialog box, type the site's address.
- 4 On the Ad Blocking tab, click **Add**.
- 5 In the Add New HTML String dialog box, select the action that you want to take.
- 6 Type an HTML string to block or permit.
- 7 Click **OK**.
- 8 When you are done, click **OK** to close the Advanced window.
- 9 Click **OK** to close the Ad Blocking window.

Modify or remove an Ad Blocking string

If you later decide that an Ad Blocking string is too restrictive, not broad enough, or not appropriate, you can change or remove it.

To modify or remove an Ad Blocking string

- 1 In the main window, double-click **Ad Blocking**.
- 2 In the Ad Blocking window, click **Advanced**.

- 3 In the left side of the Advanced window, do one of the following:
 - To modify or remove a string in the (Defaults) list, click **(Defaults)**.
 - To modify or remove a site-specific string, click the site's name.
- 4 In the HTML string list, select the string that you want to change.
- 5 Do one of the following:
 - To modify a string, click **Modify**, then type your changes.
 - To remove a string, click **Remove**.
- 6 When you are done, click **OK** to close the Advanced window.
- 7 Click **OK** to close the Ad Blocking window.

Recovering missing or erased files

16



If you purchased this product to recover files, do not install it and do not start Windows. Any new files copied to your hard disk might overwrite existing data. Starting Windows writes to your hard disk. The Windows swap file could overwrite data you would like to recover.

When you erase a file using Windows Explorer, Windows keeps a temporary copy of the file in the Recycle Bin. However, Windows does not detect files that were erased or overwritten by applications running in Windows, erased from a command prompt, or deleted via a permanent method, such as using Shift+Delete.

About Norton Protection

The Norton Protected Recycle Bin protects the following types of files:

- Files that are deleted while you are using the command line
- Files that are created and deleted by Windows applications
- Older versions of files that you modify and overwrite
- If the standard Windows Recycle Bin is not enabled, Norton Protection also protects files that would otherwise be under Recycle Bin protection

Files that are shared on a network or stored on a network server and files deleted while using your computer in DOS mode rather than Windows are not protected.

To configure Norton Protection

- 1 On the Windows desktop, right-click the **Norton Protected Recycle Bin**, then click **Properties**.
- 2 On the Norton Protection tab, make sure that Enable Protection is checked.
- 3 On the Recycle Bin tab, select the item to open when the Recycle Bin icon is double-clicked.
- 4 When you have finished, click **OK**.

See ["Use online Help"](#) on page 86.

See the context-sensitive Help to view more options in the Norton Protected Recycle Bin.

If you start your computer in DOS mode, you may find that DOS reports less free disk space than expected. This discrepancy is because DOS does not deduct the space used by deleted files protected by Norton Protection.

About UnErase Wizard

UnErase Wizard helps you recover deleted files from the Norton Protected Recycle Bin. In Windows 98/Me, UnErase Wizard can also help you restore files that were unprotected by Norton Protection. Windows 2000/XP can only recover files if Norton Protection is turned on.



If you have a dual boot system and the volume containing deleted files is not NTFS, you can use the Windows 98/Me version of UnErase Wizard to recover deleted files.

See ["Recover a file with UnErase Wizard"](#) on page 191.

Using UnErase Wizard, you can search for a deleted file by its file name and by words that you think the file may contain. This is especially useful if you can't remember the file name, but you do remember its contents.

Recover a file with UnErase Wizard



If you have excluded files from Norton Protection and these excluded files are deleted, they are not intercepted by the Windows Recycle Bin or Norton Protection and therefore are not recoverable on Windows 2000/XP systems.

UnErase Wizard displays a list of deleted files or the files that conform to file name criteria that you provide. Each file is described by its name, original location, the date it was deleted, *file type*, file size, and the program that was used to delete it. You can view the contents of a file before or after you recover it.

To see if a file is recoverable

- 1 In the center of the file list, right-click, then click **Show Unrecoverable Files**.
- 2 Click **Next**.
 Use the UnErase Wizard pages to search for and recover the files.

To recover a file with UnErase Wizard

- 1 In the main window, click **Advanced Tools**.
- 2 On the UnErase Wizard line, click **Start Tool**.
- 3 In the UnErase Wizard dialog box, select the action that you want to take. Your options are:

Find recently deleted files	Searches for the names of the most recently deleted files and displays up to a maximum of 25 deleted files (Windows 98/Me only).
Find all protected files on local drives	Searches for and displays the names of all deleted files that are protected by Norton Protection or the Windows Recycle Bin on your computer.

Find any recoverable files matching your criteria	Prompts you for search criteria. Use this option if you are looking for words that are contained in a deleted file.
Find all Norton Protected Users files	Searches for other users' protected files as well as your own. (This option is available only in Windows 2000/XP.)

- 4 Click **Next**.
UnErase Wizard displays a list of the most recently deleted files.
- 5 Select the file that you want to recover.
- 6 Click **Recover**.
If you want to examine the recovered file, make a note of the recovery destination.
- 7 If you are using Windows 98/Me and your deleted file is not listed, click **Next**.
UnErase Wizard guides you through the process of creating a more complete list of deleted files from which to select.
- 8 To close UnErase Wizard, click **Finish**.



A recovered file's name might have a question mark (?) in place of the first letter. If so, you are prompted to type the first letter of the original file name. If you do not know what it is, type any letter from A to Z as a substitute. Make a note of the file name so that you can find it later.

If you delete a file on a floppy disk from a DOS prompt by specifying file name letters after a wildcard (such as DEL *ILENAME.TXT as opposed to DEL FILENAME.TXT or DEL *.TXT), the file is listed as unrecoverable on the Recently Deleted Files page.



If you are running a recovery application such as System Restore or Norton GoBack, you must erase your history before running Wipe Info to ensure that the data is completely wiped.

About Wipe Info

When you wipe a file, Wipe Info wipes the file and attempts to wipe any free space that is associated with the file and the file's directory entry.

When you wipe a folder, Wipe Info wipes all of the files in the folder, and then, if the folder is empty, it attempts to wipe the directory entry for the folder.

In general, you cannot recover files that have been wiped. Windows Me/XP System Restore can restore files that have been wiped if they are one of the protected file types. By default, many document types, such as .doc and .xls files in My Documents, are protected. Windows Me/XP System Restore maintains copies of protected files. Wiping the original file does not wipe the copy that Windows Me/XP System Restore maintains.

Wipe Info eliminates a file's contents from the disk, but does not remove the file name. While the file name remains on disk, it is no longer visible in Windows Explorer, and there is no data stored with it. On NTFS volumes, streams (alternate data that belongs to a file but is not stored with the file) are also wiped.



Never store sensitive information in a file name or attribute. This data can be replicated throughout your system without your knowledge, for example, in a list of most recently used files, or a file name search. This type of embedded information can be very difficult to remove from your computer.

About hexadecimal values

Wipe Info uses hexadecimal values to wipe files. Hexadecimal refers to the base 16 number system. This system is used by computer programmers to represent numbers in the binary number system, which uses the zero and one symbols in combinations to represent any number.

The hexadecimal system consists of the numbers 0 to 9 and the letters A to F, used in combinations. For example, the decimal number 14 is represented as the letter E in the hexadecimal system.

In Wipe Info options, you can specify values from 00 to FF, representing numbers from 0 to 255 respectively. You can type the value using a number or a character from A to F.

About the Government Wipe process

When you select Government Wipe, Wipe Info does the following:

- Overwrites the data with 00s
- Verifies the 00 overwrite
- Overwrites with FFs
- Verifies the FF overwrite
- Writes a random value, or a value that you choose from 00 to FF
- Verifies the random overwrite

- Reverifies the random overwrite to ensure that it was written correctly
- Repeats as many times as you specify, up to 100

Set Wipe Info options

You can specify how Wipe Info handles hidden, read-only, and system files. You can also specify the type of wipe to use. The following wiping methods are available.

Fast Wipe	Overwrites the data that is being wiped with the hexadecimal value of your choice
Government Wipe	Combines several wiping and overwriting processes to conform to specifications in DoD (Department of Defense) document 5220-22-M, National Industrial Security Program Operating Manual, for the ultimate security level when eliminating data from digital media See "About the Government Wipe process" on page 194.

To change Wipe Info options

- 1 In the main window, click **Advanced Tools**.
- 2 On the Wipe Info line, click **Start Tool**.
- 3 Click **Options**.
- 4 On the General tab, select the options for Read-only, System, and Hidden file types.
- 5 On the Wipe Type tab, select one of the following:
 - Fast Wipe
 - Government Wipe
- 6 In the Hex Value text box, type the hexadecimal values that Wipe Info should use when it overwrites the wiped files space.
- 7 In the Times to Perform This Wipe text box, type the number of times that Wipe Info should repeat this process.
- 8 Click **Apply**.

See ["About hexadecimal values"](#) on page 194.

Wipe files or folders

The procedure for wiping a file varies based on the operating system on your computer. To wipe a file or folder in Windows 2000/XP, add it to the Wipe Info window.

To wipe files or folders in Windows 2000/XP

- 1 In the main window, click **Advanced Tools**.
- 2 On the Wipe Info line, click **Start Tool**.
- 3 Click **Wipe Info**.
- 4 In the Wipe Info window, click **Browse**.
- 5 Select one of the following:
 - Folders
 - Files
- 6 Select the folder or file to wipe.
- 7 Click **Open**.
- 8 With the Wipe Info window open, locate a folder or file on your hard disk.
- 9 Drag the selected item into the Wipe Info file list.
- 10 Continue to drag all of the files and folders that you want to wipe into the Wipe Info list.
If you add an item to the list by mistake, select the item, then right-click **Remove Item(s) from list**.
- 11 Click **Wipe All**.
- 12 Click **Yes** to confirm the warning.
All of the files in the list are wiped.

In Windows 98/Me, Wipe Info uses a wizard to automate the wiping process.

To wipe files or folders in Windows 98/Me

- 1 In the main window, click **Advanced Tools**.
- 2 On the Wipe Info line, click **Start Tool**.
- 3 Click **Wipe Info**.

- 4 In the Wipe Info Wizard window, select one of the following options.
Your options are:

Files	Wipe Info deletes the selected file, its directory entry if possible, and any associated free space.
Folders	Wipe Info deletes all files in the selected folder, its directory entry if possible, and any associated free space. You can specify whether subfolders should be included.
Free Space	Wipe Info wipes the free space on the selected disk. This includes free disk space, file slack space, and erased file entries that are not in the Recycle Bin. (You must empty the Recycle Bin to have deleted files wiped.) Wipe Info verifies the disk's integrity before wiping free space. If the disk has problems, you are prompted to run Norton Disk Doctor.

- 5 Select the file, folder, or disk, then click **Next**.
- 6 If you see a warning message, click **Yes** to proceed.
- 7 For Wipe Options, select one of the following:
- Fast Wipe
 - Government Wipe
- 8 If you want to change any selections, click **Back**.
Wipe Info displays its progress and summarizes the results, including any problems that were encountered during the wiping process.
- 9 In the Wipe Summary window, review what Wipe Info will do, then click **Next**.
- 10 View the results, then click **Close**.
- 11 Follow the on-screen instructions to finish the wiping process.

See ["Set Wipe Info options"](#) on page 195.



Improving Web browsing and connectivity

18

There are two programs that make your Internet activities more efficient and reliable. Web Cleanup lets you quickly and safely delete the files and data that accumulate after you browse the Internet. Connection Keep Alive lets you maintain your *dial-up* Internet connection even when you're not actively using the connection.

About Web Cleanup

Web Cleanup locates and deletes temporary files and data items that collect on your computer after you browse the Internet with Internet Explorer. These items accumulate in your computer's Internet history and temporary *cache* file storage areas. Most of these temporary files have little value, occupy disk space, and slow down your computer's performance.



Web Cleanup works only with Internet Explorer and its associated files.

Web Cleanup lets you view the contents of files before you delete them. You can add *domain names*, or URLs, to a list so that Web Cleanup doesn't select them for deletion again.

Certain types of files, such as *cookies*, store personal data. You might want to keep these files to save the effort of repeatedly logging onto a frequently used, secure site. However, this personal data could be the target of hackers or other malevolent programmers.

With Web Cleanup, you can:

- Automatically delete all unnecessary Web files and related data items with Quick Clean.
- View individual files and other Internet items to save or delete with Advanced Cleanup.

Delete unnecessary Web files

Quick Clean scans for files that are typically left behind after Internet browsing. These include Internet history and *cache* files, and *cookies*. At the completion of the scan, you have the option to delete all of the files that were found during the scan.

See "View Web Cleanup files" on page 200.

If you want to see more information about the files before they are deleted, you can select them individually using Advanced Cleanup.

To delete unnecessary Web files

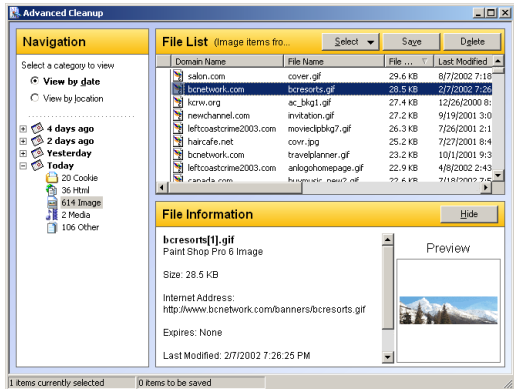
- 1 In the Security Center, click **Web Tools > Web Cleanup**.
- 2 Click **Begin Quick Clean**.
Quick Clean scans your computer and displays a summary of files and other Internet items that can be deleted.
- 3 Click **Cleanup Now!** to delete all of the summarized items automatically.
- 4 Click **Finish**.

View Web Cleanup files

Web Cleanup lets you view detailed information about all of the files that are selected for deletion. You can view a selected file's creation date, type, contents, and other information. Viewing information helps you determine if a file should be deleted or saved.

To view Web Cleanup files

- 1 In the Security Center, click **Web Tools > Web Cleanup**.
- 2 Click **Advanced Cleanup**.



- 3 In the Navigation pane, select how to display the grouped categories. Your options are:

View by date	File categories are listed chronologically with the most recently viewed Web site files listed first.
View by location	File categories are listed alphanumerically by the associated Web site domain name, IP address, or other identifying name.

- 4 In the Navigation pane, click the plus sign next to a Web site or category (History, HTML, image, cookie) to display its contents.
- 5 Click an item.
- 6 Under Domain Name, click a file category to display individual files in the File List.
- 7 To close the File Information pane and view more items in the File List, click **Hide**.

- 8
- To sort the File List, click a column heading.
Expand the window or use the horizontal scroll bar to see more columns. The columns include the following information:

Domain Name	Web site name or URL
File Name	File name on the disk
File Size	The size in bytes on your hard disk
Last Modified	The date when the file was last changed on the hard disk
Expires	If the file is a cookie, the date when it expires
Last Sync	If the file is a synchronized file, the date when the item was last synchronized with another device (such as a handheld device)
Last Accessed	The date when the domain name was last accessed from your computer

- 9
- In the File List, select an item to display more information in the File Information pane.
If you closed the File Information pane, click **Show**.
- 10
- In the File List, select one or more items using one of the commands on the Select menu.

- 11 Identify what to do with the selected items. Your options are:

Save	Add the item to the Web Cleanup tab in the Web Tools Options dialog box. Domains in this list will not be deleted by Quick Clean.
Delete	Remove the selected file from the Viewer List, but do not delete the file. It will show up in the scan next time, unless you add it to the list of excluded Web sites in the Web Cleanup Options list.

If you saved a domain name, in the alert message, click **OK**.

- 12 When you are finished, close the View Files window.

Exclude domains from Web Cleanup activity

You can list Web *domain names* whose files should be excluded from Web Cleanup activity. Along with the domain names, you can specify which categories of files, *cookies*, *cache*, or history, should be protected.

It might help to have your Internet browser open to a Web site's home page as you are typing, so that you can refer to the correct spelling of the domain name in your browser's address line.

You can type the domain names directly in the Web Cleanup dialog box. You can also select them in the Advanced Cleanup file list.

To exclude domain names in the Web Cleanup list

- 1 On the Options menu, click **Web Tools**.
- 2 In the Web Cleanup dialog box, click **Insert**.

- 3
- Type the domain name that you want to exclude from deletion, then press **Enter**.
For example, type `www.symantec.com` to add the Symantec Web site to the list.
- 4
- For the domain, select the types of files that you want to exclude from Web Cleanup activity. Your options are:

Cookies	Any cookies that are associated with the domain
Cache	Any cache files that are associated with the domain
History	Any history files of Internet activity that include the domain name

- 5
- Click **Apply**.
- 6
- Repeat steps 2 to 5 until you have added all of the domain names that you want to exclude from Web Cleanup activity.
- 7
- Click **OK**.

To exclude domain names in the Advanced Cleanup File List

- 1
- In the Security Center, click **Web Tools > Web Cleanup**.
- 2
- In the Web Cleanup main window, click **Advanced Cleanup**.
- 3
- In the Advanced Cleanup window, in the File List, select one or more items using one of the commands on the Select menu.
- 4
- Click **Save**.
The domain name is added to the list of domains in the Web Cleanup dialog box.
All file categories for the domain, including cookies, cache, and history, are checked.
- 5
- Repeat steps 3 to 4 until you have selected all of the domain names that you want to exclude from Web Cleanup activity.

About Connection Keep Alive

Connection Keep Alive prevents your *dial-up* Internet connection from disconnecting when you want to stay connected, but are not browsing the Internet, using email, or performing another Internet activity. Connection Keep Alive sends a small signal to a Web site. This prevents your Internet service provider (*ISP*) from canceling the connection.



Some ISPs might not allow this activity. Read your ISP's User Agreement before you enable Connection Keep Alive.

Enable or disable Connection Keep Alive

You can enable Connection Keep Alive whenever you need it. You can also specify how long you want to stay connected before Connection Keep Alive quits.

You can enable or disable Connection Keep Alive from the Security Center or from the Windows system tray.

To enable or disable Connection Keep Alive from the Security Center

- 1 In the Security Center, click **Web Tools > Connection Keep Alive**.
The Connection Keep Alive status indicates whether it is On or Off.
- 2 Select one of the following:
 - Enable
 - Disable

To enable or disable Connection Keep Alive from the system tray

- 1 In the Windows system tray, right-click the Connection Keep Alive icon.
- 2 Select one of the following:
 - Enable Connection Keep Alive
 - Disable Connection Keep Alive

View Connection Keep Alive status

After you have used Connection Keep Alive for the first time, you can view whether it is enabled or disabled in the following ways:

- When it is disabled, the Connection Keep Alive Windows system tray icon has a small X.
- Hold the mouse cursor over the Connection Keep Alive icon. A tooltip displays its status.
- In the Security Center, the Connection Keep Alive panel indicates its status as ON (enabled) or OFF (disabled).


Set Connection Keep Alive options

You can specify if Connection Keep Alive should start when Windows starts, the level of activity it uses, the Web sites to which it sends signals, and when to stop sending signals. You can access Connection Keep Alive options from the Security Center or from the Windows System tray.

To set Connection Keep Alive options from the Security Center

- 1 In the Security Center, click **Options > Web Tools**.
- 2 On the **Connection Keep Alive** tab, change the settings. Your options are:

Automatically start with Windows	Connection Keep Alive is enabled when Windows starts.
Display splash screen on startup	Connection Keep Alive displays a splash screen when Windows starts.

Keep Alive Level Low/High	<p>The frequency with which Connection Keep Alive sends signals to (pings) its network. For UDP and ICMP network communications protocols, the Low or High settings can be used. For the HTTP communications protocol, only the High setting is used.</p>
Network traffic destination My Favorites My Homepage <ping.symantec.com>	<p>When it simulates network traffic, Connection Keep Alive pings the Web sites in My Favorites, My Homepage, the Symantec Web site, or ping.symantec.com. You can replace ping.symantec.com with your own choice.</p> <p> If the Keep Alive Level is set to High, and you specify a different Web site to ping, be sure to include the HTTP prefix, for example http://www.myownurl.com</p>
Simulate network activity every XX minute(s)	<p>Connection Keep Alive sends a signal every 1, 2, 3, or more minutes, up to 15. The default is 1 minute.</p>

Disable when inactive for more than XX minute(s)	If there is no mouse or keyboard activity, Connection Keep Alive disables itself after the indicated period.
Display timeout warning message	Connection Keep Alive displays a warning message before it disables itself after the scheduled number of minutes. The message remains for a countdown of 60 seconds. If you respond to the message, Connection Keep Alive remains active.

- 3 When you are finished, click **OK**.

To set Connection Keep Alive options from the Windows system tray

- 1 In the Windows system tray, right-click the Connection Keep Alive icon, then click **Connection Keep Alive Options**.
- 2 In the Connection Keep Alive Options dialog box, change the settings.
- 3 Click **OK**.

Monitoring Norton Internet Security Professional

19

Norton Internet Security Professional maintains records of all incoming and outgoing Internet connections and any actions that the program takes to protect your computer. You should periodically review this information to spot potential problems.



Each copy of Norton Internet Security Professional maintains a separate set of logs and statistics. If you have more than one copy of Norton Internet Security Professional, you will need to check each computer's records individually.

There are several sources of information:

Status & Settings window	Basic information about which protection features are active
Statistics window	Recent information about firewall and content-blocking activities
Detailed statistics window	Detailed information about network activity and actions that Norton Internet Security Professional has taken
Event Log	Internet activities and any actions Norton Internet Security Professional has taken

View the Statistics window

The Statistics window provides a snapshot of your computer's network activity since the last time you started Windows. Use this information to identify ongoing attack attempts and review how your Privacy Control and Productivity Control settings affect your protection.

The Statistics window includes information on the following:

Personal Firewall	Any recent attacks on this computer, including the time of the most recent attack and the address of the attacking computer
Online Content Blocking	The number of cookies, images, and other online content that has been blocked and the number of times private information has been blocked
Productivity Control	Web sites and programs that have been blocked

To view the Statistics window

- ❖ In the main window, click **Statistics**.

Reset information in the Statistics window

The statistics in the Statistics window are automatically cleared when you restart Windows. You can also clear the statistics manually. This helps you see if a configuration change affects the statistics.

To reset information in the Statistics window

- 1 In the main window, click **Statistics**.
- 2 In the Statistics window, click **Clear Statistics**.

Review detailed statistics

Along with the overall statistics in the Statistics window, Norton Internet Security Professional maintains real-time network counters that track users' Internet usage and any actions that the program takes.

The detailed statistics include the following information:

Network	TCP and UDP bytes sent and received, the number of open network connections, and the highest number of simultaneous open network connections since the program started
Online content	The number of graphics, cookies, spam, and private information that have been blocked and the number of open HTTP connections
Firewall TCP Connections	The number of blocked and permitted TCP connections
Firewall UDP Datagrams	The number of blocked and permitted UDP connections
Firewall Rules	All of the rules defined for your firewall and information on the number of communication attempts blocked, permitted, or not matched by firewall rules
Network Connections	Information about current connections, including the program that is using the connection, the protocol being used, and the addresses or names of the connected computers
Last 60 Seconds	The number of network and HTTP connections and the speed of each connection type

To review detailed statistics

- 1 In the main window, click **Statistics**.
- 2 In the Statistics window, click **Detailed Statistics**.

View Norton Internet Security Professional logs

Norton Internet Security Professional records information about Web sites that users have visited, actions that the firewall has taken, and any alerts that have been triggered. The logs include details about some of the activity reported in the Statistics window.

Review log information

View the Norton Internet Security Professional logs from the Statistics window.

To view the logs

- 1 In the main window, click **Statistics > View Logs**.
- 2 In the Log Viewer, in the left pane, select the log that you want to review. Your options are:

Content Blocking	Details about ads, Java applets, ActiveX controls, scripts, Flash animations, and GIF animations blocked
Connections	A history of all TCP/IP network connections made with this computer, including the date and time of the connection, the address of the computer to which you connected, the service or port number used, the amount of information transferred, and the total time the connection was active
Firewall	Communication intercepted by the firewall, including rules that were processed, alerts displayed, unused ports blocked, and AutoBlock events

Intrusion Detection	Whether Intrusion Detection is active, attack signatures being monitored, and the number of intrusions blocked
Privacy	The cookies that have been blocked, including the name of the cookie and the Web site that requested the cookie
Private Information	A history of all protected private information sent over the Internet
System	Severe system errors, the current status of IP filtering, if the logged program started as a Windows service, and information about programs that are using too many resources or otherwise operating under less than optimum conditions
Web History	URLs visited by the computer, providing a history of Web activity
Alerts	Any security alerts triggered by possible attacks on your computer
Restrictions	The Internet programs, newsgroups, and Web sites blocked by Productivity Control
Norton AntiSpam	Details about emails identified as spam

As you click each log, the right pane changes and displays details specific to the particular log. The most recent activities appear at the top of the log.

- 3 When you are finished viewing the information, click **File > Exit**.

Monitor Norton AntiVirus activities

Occasionally, you may need to look at previous Norton AntiVirus activities, such as when the last system scan was done or how many viruses were detected last week. Norton AntiVirus displays a record of its threat detection, application, and error activities in the Log Viewer.

About the Log Viewer

The Log Viewer displays the history of activities in each Activity Log. An Activity Log is a collection of multiple log files, one for each type of information collected: threat alerts, application activities, and errors.

Using the information in the Log Viewer, you can:

- View detailed information recorded in each log by selecting the log in the left column and viewing the details in the right pane.
- Delete the activity entries for a log by selecting the log, then clicking Clear. If you never clear the entries for a category, it expands until it reaches the maximum size. Then it starts overwriting the oldest entries.

Check the Activity Log

Check the Activity Log to see what tasks were performed and the results of those tasks to make sure that your Options settings are appropriate for your particular needs.

To check the Activity Log

- 1 In the main window, under Norton AntiVirus, click **Reports**.
- 2 In the Reports pane, on the Activity Log line, click **View Report**.

- 3 In the left pane, select the log that you want to review. Your options are:

Threat alerts	A history of threat alerts, such as the ID and type of threat, date and time when it occurred, the action taken, and the version of the virus definitions used.
Application activities	A history of scanning activities, such as when scanning occurred and with what results.
Errors	Detailed information about any problems encountered when scanning your computer such as the date, error code, and message.

As you select each log, the right pane changes and displays details specific to the particular log. The most recent activities appear at the top of the log.

- 4 When you are finished viewing the information, click **File > Exit**.



The information in this chapter will help you solve the most frequently encountered problems. If you can't find the solution to your problem here, there is a wealth of information on the Symantec Web site.

Explore the Symantec service and support Web site

On the Symantec service and support Web site, you can find the latest protection and program updates, patches, online tutorials, Knowledge Base articles, and virus removal tools.

To explore the Symantec service and support Web site

- 1 On the Internet, go to www.symantec.com/techsupp
- 2 On the service and support Web page, under the heading home & home office/small business, click **Continue**.
- 3 On the home & home office/small business page, click **start online support**.
- 4 Follow the links to the information that you want.

If you cannot find what you are looking for using the links on the introduction page, try searching the Web site.

To search the Symantec service and support Web site

- 1 On the left side of any Symantec Web site page, click **search**.

- 2 On the search page, type a word or phrase that best represents the information for which you are looking. Use the following guidelines when searching the Symantec Web site:
 - Type a single word in lowercase letters to find all occurrences of the word, including partial matches. For example, type `install` to find articles that include the word `install`, `installation`, `installing`, and so on.
 - Type multiple words to find all occurrences of any of the words. For example, type `virus definitions` to find articles that include `virus` or `definitions` or both.
 - Type a phrase enclosed in quotation marks to find articles that include this exact phrase.
 - Type a plus (+) sign in front of all of the search terms to retrieve documents containing all of the words. For example, `+Internet +Security` finds articles containing both words.
 - For an exact match, type the search words in uppercase letters.
 - To search for multiple phrases, enclose each phrase in quotation marks and use commas to separate the phrases. For example, `"purchase product", "MAC", "Norton SystemWorks"` searches for all three phrases, and finds all articles that include any of these phrases.
- 3 Select the area of the Web site that you want to search.
- 4 Click **Search**.

Troubleshoot Norton Internet Security Professional

Check here for possible solutions to issues that might arise with Norton Internet Security Professional.

What is wrong with this Web site?

If you cannot connect to a Web site with Norton Internet Security Professional disabled, there might be a problem with the Internet or your [Internet service provider](#). If your connection is working, it's possible a Norton Internet Security Professional feature is preventing you from viewing the site.

Problem	Solution
It could be Cookie Blocking	<p>Many Web sites require that cookies be enabled on your computer to display correctly.</p> <p>See "Change the Cookie Blocking setting" on page 179.</p>
It could be a firewall rule	<p>A firewall rule might be blocking the Web site. When this happens, you will usually see a message saying that you could not connect.</p> <p>See "Customize firewall protection" on page 112.</p>
It could be Ad Blocking	<p>Sometimes blocking advertisements on the Internet prevents an entire Web site from appearing in your browser.</p> <p>See "Blocking Internet advertisements" on page 185.</p>
It could be ActiveX or Java blocking	<p>Some Web sites display only ActiveX controls or Java applets. If you are blocking them, nothing appears on these sites.</p> <p>See "Change individual security settings" on page 112.</p>

Why can't I post information online?

See ["Modify or remove private information"](#) on page 176.

If you are unable to post information to a Web site, it may be because Privacy Control is blocking the information. Check the Private Information list to see if the information that you are trying to enter is being blocked.

Why did an email message I sent never arrive?

If you choose to block an email message containing private information, Norton Internet Security Professional immediately deletes the email message. Your email program will indicate that the message was sent, but the recipient will not receive it.

If your email program maintains copies of sent messages in its Sent or Out folder, you can reopen the email message, remove the private information, and send the message again.

Why doesn't Norton Internet Security Professional notify me before letting programs access the Internet?

See ["Enable Automatic Program Control"](#) on page 116.

If Automatic Program Control is on, Norton Internet Security Professional creates rules for programs that it recognizes without notifying you.

Why can't I print to a shared printer or connect to a computer on my local network?

Norton Internet Security Professional blocks the use of Microsoft networking to prevent someone from connecting to your computer over the Internet.

See ["Allow or block access to your computer"](#) on page 114.

To allow the use of your local network, including file and printer sharing, place the computers on your local network in the Trusted Zone.

How can a Web site get my browser information?

The Browser Privacy settings prevent your browser from sending browser information. However, some diagnostic sites on the Internet might report browser information even though the Browser Privacy settings are blocking it.



Troubleshoot Norton AntiSpam

This information will help you solve the most frequently encountered problems with Norton AntiSpam.

Why do I still receive spam?

Several factors make it difficult to completely eliminate spam. For example, different people will consider different classes of email messages to be unwelcome or intrusive. Some, for instance, do not want to receive anything they have not specifically requested. Others are glad to receive items regarding their interests or profession even if they have not specifically requested them.

How will email messages from addresses on my Blocked list be handled?

Norton AntiSpam moves email messages from these addresses to the Norton AntiSpam folder and marks them in the subject line as spam.

What if I mistakenly put an address on the Blocked list?

The only result will be that you will not see any email messages from this address in your main list. But if you periodically review the contents of your spam folder, you will be able to retrieve any email messages from that address and then correct the entry in your list.

Why did an email message someone sent me never arrive?

Some legitimate email messages may contain elements that are characteristic of spam messages. This may have caused Norton AntiSpam to incorrectly identify the message as spam. Depending upon the filters you have created in your email program, the message may be in your spam or trash folder.

See ["Identify authorized senders"](#) on page 67.

To avoid losing email messages from this person, add them to your Allowed list.

How do I keep my protection updated?

To some degree, Norton AntiSpam updates itself by learning from your outgoing email messages and other data. However, to receive up-to-date copies of Symantec spam definitions, you must subscribe to this service. You can then choose to have these definitions updated automatically.

Why do I need a subscription to spam definitions?

Though the product is self-training, local spam definitions are developed only by the criteria you input and from the sample of email messages you process. Symantec spam definitions are developed from a much larger set of information and can prevent you from seeing many of the more common types of spam.

Why does so much spam include clusters of meaningless characters?

These and other unusual elements in spam are intended to confuse spam filters that look for keywords.



Troubleshoot Ad Blocking

This information will help you solve the most frequently encountered problems with Ad Blocking.

Does Ad Blocking block all advertising on the current page?

Ads that are integrated with standard content—for instance text statements—will not be blocked.

Will Popup Window Blocking block all pop-ups or only pop-up ads?

Ad Blocking blocks all pop-ups that are started automatically during a Web page load. If a site uses pop-ups for special alerts or additional information, you might want to disable Popup Window Blocking while viewing that site.

Are there security issues associated with advertisements?

While clicking on an ad should only display more information or direct you to another site, some advertisers will use ads to entice you into installing new functionality on your system. These may range from adding new menus to installing spyware. You should be especially wary of ads that invite you to install novelty cursors or other entertaining add-ons. These frequently include user agreements that require you to allow companies to track your browsing or to provide them with personal information, among other things. Such clauses are typically hidden deep in the text where many users will not bother to read them.

Troubleshoot Norton AntiVirus

Check here for possible solutions to issues that might arise with Norton AntiVirus.

Auto-Protect does not load when I start my computer

If the Norton AntiVirus Auto-Protect icon does not appear in the lower-right corner of the Windows taskbar, Auto-Protect is not loaded. There are three likely reasons that this is happening.

You may have started Windows in safe mode. Windows restarts in safe mode if the previous shutdown did not complete successfully. For example, you may have turned off the power without choosing Shut Down on the Windows Start menu.

To restart Windows

- 1 On the Windows taskbar, click **Start > Shut Down**.
- 2 In the Shut Down Windows dialog box, click **Restart**.
- 3 Click **OK**.

Norton AntiVirus may not be configured to start Auto-Protect automatically.

To set Auto-Protect to start automatically

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under System, click **Auto-Protect**.
- 3 Ensure that Start Auto-Protect when Windows starts up is checked.

Norton AntiVirus may not be configured to show the Auto-Protect icon in the tray.

To show the Auto-Protect icon in the tray

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under System, click **Auto-Protect**.
- 3 Ensure that Show the Auto-Protect icon in the tray is checked.

I have scanned and removed a virus, but it keeps infecting my files

There are four possible reasons a virus could be reappearing.

The virus might be in a program file with an unusual extension for which Norton AntiVirus is not configured to look.

To reset Norton AntiVirus scanning options

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under System, click **Manual Scan**.
- 3 Under Which file types to scan for viruses, click **Comprehensive file scanning**.
- 4 Click **Manual Scan > Bloodhound**.
- 5 Ensure that Enable Bloodhound heuristics is checked, then click **Highest level of protection**.
- 6 Click **OK**.
- 7 Scan all of the disks that you use and repair all infected files.

The source of the infection could also be a floppy disk. Scan all of the floppy disks that you use to ensure that they are free of viruses.

See "If you need to use Rescue Disks to restore your system" on page 84.

Another reason could be that the virus is remaining in memory after you remove it from the *boot record*. It then reinfects your boot record. Use your Rescue Disks to remove the virus.

If the problem is a Trojan horse or worm that was transmitted over a shared network drive, you must

disconnect from the network or password protect the drive to let Norton AntiVirus delete the problem.

Norton AntiVirus cannot repair my infected files

See ["Keeping current with LiveUpdate"](#) on page 103.

The most common reason that Norton AntiVirus cannot repair your infected files is that you do not have the most current virus protection on your computer. Update your virus definitions regularly to protect your computer from the latest viruses.

If after using LiveUpdate the virus still cannot be repaired, the file may be corrupted, or contain a new virus. There are two additional options:

See ["If Norton AntiVirus places files in Quarantine"](#) on page 152.

- Quarantine the file and submit it to Symantec.
- If you don't need the file or a non-infected copy of the file exists, delete the infected file and replace it with the non-infected file.

I can't receive email messages

There are several possible solutions to this problem.

If you are using a firewall, it may block access to the Internet features of Norton AntiVirus.

Temporarily disable email protection. This might allow the problem email messages to download so that you can once again enable email protection. You are protected by Auto-Protect while email protection is disabled.

To temporarily disable incoming email protection

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under Internet, click **Email**.
- 3 Uncheck **Scan incoming Email**.
- 4 Click **OK**.
- 5 Download your email messages.
- 6 Reenable incoming email protection.

See ["About System options"](#) on page 96.

Your email client may have timed out. Make sure that timeout protection is enabled.

If you continue to experience problems downloading email messages, disable email protection.

To disable email protection

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under Internet, click **Email**.
- 3 Uncheck **Scan incoming Email**.
- 4 Uncheck **Scan outgoing Email**.
- 5 Click **OK**.

I can't send email messages

If you get the message Norton AntiVirus was unable to send your email message because the connection to your email server was disconnected, your email client may be set to automatically disconnect after sending and receiving mail.

If you are using a firewall, it may block access to the Internet features of Norton AntiVirus.

For Norton AntiVirus to scan outgoing email messages for viruses, it intercepts and scans the messages before they are sent to your email provider. To resolve this issue, turn off this option within your email client. Consult your email client manual for instructions on how to do this, or disable Norton AntiVirus outgoing email scanning.

To disable outgoing email scanning

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under Internet, click **Email**.
- 3 Uncheck **Scan outgoing Email**.
- 4 Click **OK**.

Troubleshoot Rescue Disks

Check here for possible solutions to issues that might arise with Rescue Disks.

My Rescue Disk does not work

See ["Create and use Rescue Disks"](#) on page 80.

Due to the number of product-specific technologies used by manufacturers to configure and initialize hard drives, the Rescue program cannot always create a bootable disk automatically. If your Rescue Boot Disk does not work properly, do one of the following:

- Be sure you have downloaded the latest Rescue Disk update from LiveUpdate.
- If you have a special startup disk for your computer, add it to your Rescue Disk set. In an emergency, start from that disk. Remove the disk and insert your Rescue Boot Disk. At the DOS prompt, type **A:RSHELL**, press Enter, then follow the on-screen instructions.
- Use the Disk Manager or similarly named program that came with your computer to make your Rescue Boot Disk bootable. Make sure to test your modified Rescue Boot Disk.

Sometimes, your Rescue Boot Disk does not work properly because you have more than one operating system installed, such as Windows 2000 and Windows 98.

To modify your Rescue Boot Disk

- 1 Start up from your hard drive.
- 2 Insert your Rescue Boot Disk into drive A.
- 3 At the DOS prompt, type **SYS A:**
- 4 Press **Enter**.
 This transfers the operating system to the Rescue Boot Disk. Be sure to retest your Rescue Disks.

I cannot start from drive A

See [“Create and use Rescue Disks”](#) on page 80.

If your computer does not check drive A first on startup, use your computer's Setup program to change settings.

Be careful when making changes using your computer's Setup program. If you have never used it before, you may want to refer to your computer manufacturer's documentation.

To change your computer's settings

- 1 Restart your computer.
A message appears telling you the key or keys to press to run SETUP, such as Press if you want to run SETUP.
- 2 Press the key or keys to launch the Setup program.
- 3 Set the Boot Sequence to boot drive A first and drive C second.
Setup programs vary from one manufacturer to the next. If you cannot find the Boot Sequence option, use the Setup program's Help system, refer to the documentation that came with your system, or contact your system's manufacturer.
- 4 Save the changes, then exit the Setup program.

You may need to use a special boot disk rather than the Rescue Boot Disk. In this case, use the boot disk or startup disk that came with your computer.

See [“My Rescue Disk does not work”](#) on page 229.

If your computer is set up with more than one operating system, such as Windows 2000 and Windows 98, you may need to modify the Rescue Boot Disk.

I get an error when testing basic Rescue Disks

See [“Create and use Rescue Disks”](#) on page 80.

If you get the message Non-system disk, replace the disk and press any key when testing your Rescue Disks, the Rescue program may not have prepared the floppy boot files correctly.

To repair the Rescue Boot Disk without having to reformat the disk and create a new Rescue Disk set

- 1 Remove the Rescue Boot Disk and restart your computer.
- 2 Insert the Rescue Boot Disk into the floppy disk drive.
- 3 On the Windows taskbar, click **Start > Run**.
- 4 In the Run dialog box, type **SYS A:**
- 5 Click **OK**.



Service and support solutions

The Service & Support Web site at <http://service.symantec.com> supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

Customer service

The Service & Support Web site at <http://service.symantec.com> tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Replace defective CD-ROMs and manuals.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at:
<http://www.symantecstore.com>

Technical support

Symantec offers two technical support options for help with installing, configuring, or troubleshooting Symantec products:

- **Online Service and Support**
Connect to the Symantec Service & Support Web site at <http://service.symantec.com>, select your user type, and then select your product and version. You can access hot topics, Knowledge Base articles, tutorials, contact options, and more. You can also post a question to an online Technical Support representative.
- **PriorityCare telephone support**
This fee-based (in most areas) telephone support is available to all registered customers. Find the phone number for your product at the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options.

Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued 60 days later. Technical information may still be available through the Service & Support Web site at:
<http://service.symantec.com>

Subscription policy

If your Symantec product includes virus, firewall, or Web content protection, you may be entitled to receive updates via LiveUpdate. Subscription length varies by Symantec product.

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web

content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to <http://service.symantec.com> and select your region under Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

<http://www.symantec.com/>

Australia and New Zealand

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Europe, Middle East, and Africa

Symantec Authorized Service Center
Postbus 1029
3600 BA Maarssen
The Netherlands

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Latin America

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12º andar
São Paulo – SP
CEP: 04583-904
Brasil, SA

Portuguese:
<http://www.service.symantec.com/br>
Spanish:
<http://www.service.symantec.com/mx>
Brazil: +55 (11) 5189-6300
Mexico: +52 55 5322 3681 (Mexico DF)
01 800 711 8443 (Interior)
Argentina: +54 (11) 5382-3802

June 3, 2003

Glossary

access privileges	The types of operations that a user can perform on a system resource. For example, a user can have the ability to access a certain directory and open, modify, or delete its contents.
ActiveSync	The synchronization software for Microsoft Windows-based Pocket PCs.
ActiveX	A method of embedding interactive programs into Web pages. The programs, which are called controls, run when you view the page.
alert	A message that appears to signal that an error has occurred or that there is a task that requires immediate attention, such as a system crash or a Virus Alert.
alias	A shortcut icon that points to an original object such as a file, folder, or disk.
AppleTalk	A protocol that is used by some network devices such as printers and servers to communicate.
attack signature	A data pattern that is characteristic of an Internet attack. Intrusion Detection uses attack signatures to distinguish attacks from legitimate traffic.
beam	To transfer certain programs and data between two handheld devices using built-in infrared technology.

boot record	A sector at the start of a disk that describes the disk (sector size, cluster size, and so on). On startup disks, the boot record also has a program that loads the operating system.
bootable disk	A disk that can be used to start a computer.
cache	A location on your disk in which data is stored for reuse. A Web browser cache stores Web pages and files (such as graphics) as you view them.
cache file	A file that is used to improve the performance of Windows.
compressed file	A file whose content has been made smaller so that the resulting data occupies less physical space on the disk.
connection-based protocol	A protocol that requires a connection before information packets are transmitted.
connectionless protocol	A protocol that sends a transmission to a destination address on a network without establishing a connection.
cookie	A file that some Web servers put on your disk when you view pages from those servers. Cookies store preferences, create online shopping carts, and identify repeat visitors.
denial-of-service attack	A user or program that takes up all of the system resources by launching a multitude of requests, leaving no resources, and thereby denying service to other users.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that assigns a temporary IP address to each device on a network. DSL and cable routers use DHCP to allow multiple computers to share a single Internet connection.
dial-up	A connection in which a computer calls a server and operates as a local workstation on the network.

DNS (Domain Name System)	The naming system used on the Internet. DNS translates domain names (such as www.symantec.com) into IP addresses that computers understand (such as 206.204.212.71).
DNS server (Domain Name System server)	A computer that maps domain names to IP addresses. When you visit www.symantec.com , your computer contacts a DNS server that translates the domain name into an IP address (206.204.212.71).
domain	The common Internet address for a single company or organization (such as symantec.com). See also host name.
DOS window	A method of accessing the MS-DOS operating system to execute DOS programs through the Windows graphical environment.
download	To transfer a copy of a file or program from the Internet, a server, or computer system to another server or computer.
driver	Software instructions for interpreting commands for transfer to and from peripheral devices and a computer.
encryption	Encoding data in such a way that only a person with the correct password or cryptographic key can read it. This prevents unauthorized users from viewing or tampering with the data.
Ethernet	A common method of networking computers in a LAN (local area network). Ethernet cables, which look like oversized phone cables, carry data at 10M bps or 100M bps.
executable file	A file containing program code that can be run. Generally includes any file that is a program, extension, or system files whose names end with .bat, .exe, or .com.

extension	The three-letter ending on a file name that associates the file with an activity or program. Examples include .txt (text) and .exe (executable program).
FAT (file allocation table)	A system table (used primarily by DOS and Windows 9x/Me) that organizes the exact location of the files on the hard drive.
file type	A code that associates the file with a program or activity, often appearing as the file name extension, such as .txt or .jpeg.
Finder	The program that manages your Macintosh disk and file activity and display.
firewall rule	Parameters that define how a firewall reacts to specific data or network communications. A firewall rule usually contains a data pattern and an action to take if the pattern is found.
fragmented	When the data that makes up a file is stored in noncontiguous clusters across a disk. A fragmented file takes longer to read from the disk than an unfragmented file.
fragmented IP packet	An IP packet that has been split into parts. Packets are fragmented if they exceed a network's maximum packet size, but malicious users also fragment them to hide Internet attacks.
FTP (File Transfer Protocol)	An application protocol used for transferring files between computers over TCP/IP networks such as the Internet.
hidden attribute	A file attribute that makes files harder to access and more difficult to delete than other files. It also prevents them from appearing in a DOS or Windows directory list.

host name	The name by which most users refer to a Web site. For example, www.symantec.com is the host name for the Symantec Web site. Host names are translated to IP addresses by the DNS.
HotSync	The synchronization software for Palm OS handheld devices.
HTML (Hypertext Markup Language)	The language used to create Web pages.
ICMP (Internet Control Message Protocol)	An extension to the basic Internet Protocol (IP) that provides feedback about network problems.
IGMP (Internet Group Management Protocol)	An extension to the basic Internet Protocol (IP) that is used to broadcast multimedia over the Internet.
IMAP4 (Internet Message Access Protocol version 4)	One of the two most popular protocols for receiving email. IMAP makes messages available to read and manage without downloading them to your computer.
infrared (IR) port	A communication port on a handheld device for interfacing with an infrared-capable device. Infrared ports do not use cables.
IP (Internet Protocol)	The protocol that underlies most Internet traffic. IP determines how data flows from one computer to another. Computers on the Internet have IP addresses that uniquely identify them.
IP address (Internet Protocol address)	A numeric identifier that uniquely identifies a computer on the Internet. IP addresses are usually shown as four groups of numbers separated by periods. For example, 206.204.52.71.
ISP (Internet service provider)	A company that supplies Internet access to individuals and companies. Most ISPs offer additional Internet connectivity services, such as Web site hosting.

Java	A programming language used to create small programs called applets. Java applets can be used to create interactive content on Web pages.
JavaScript	A scripting language used to enhance Web pages. Most sites use JavaScript to add simple interactivity to pages, but some use it to open pop-up ads and reset visitors' homepages.
macro	A simple software program that can be started by a specific keystroke or a series of keystrokes. Macros can be used to automate repetitive tasks.
NAT (network address translation)	A method of mapping private IP addresses to a single public IP address. NAT allows multiple computers to share a single public IP address. Most DSL and cable routers support NAT.
network address	The portion of an IP address that is shared by all computers on a network or subnet. For example, 10.0.1.1 and 10.0.1.8 are part of the network address 10.0.1.0.
NTFS (NTFS file system)	A system table (used primarily by Windows 2000/XP) that organizes the exact location of all the files on the hard drive.
packet	The basic unit of data on the Internet. Along with the data, each packet includes a header that describes the packet's destination and how the data should be processed.
partition	A portion of a disk that is prepared and set aside by a special disk utility to function as a separate disk.
POP3 (Post Office Protocol version 3)	One of the two most popular protocols for receiving email. POP3 requires that you download messages to read them.
port	A connection between two computers. TCP/IP and UDP use ports to indicate the type of server program that should handle a connection. Each port is identified by a number.

port number	A number used to identify a particular Internet service. Internet packets include the port number to help recipient computers decide which program should handle the data.
PPP (Point-to-Point Protocol)	A protocol for communication between two computers using a dial-up connection. PPP provides error-checking features.
protocol	A set of rules governing the communication and transfer of data between computers. Examples of protocols include HTTP and FTP.
proxy	A computer or program that redirects incoming and outgoing traffic between computers or networks. Proxies are often used to protect computers and networks from outside threats.
registry	A category of data stored in the Windows registry that describes user preferences, hardware settings, and other configuration information. Registry data is accessed using registry keys.
removable media	Disks that can be removed, as opposed to those that cannot. Some examples of removable media are floppy disks, CDs, DVDs, and Zip disks.
router	A device that forwards information between computers and networks. Routers are used to manage the paths that data takes over a network. Many cable and DSL modems include routers.
script	A program, written in a scripting language such as VBScript or JavaScript, that consists of a set of instructions that can run without user interaction.
service	General term for the process of offering information access to other computers. Common services include Web service and FTP service. Computers offering services are called servers.

SSL (Secure Sockets Layer)	A protocol for secure online communication. Messages sent using SSL are encrypted to prevent unauthorized viewing. SSL is often used to protect financial information.
subnet	A local area network that is part of a larger intranet or the Internet.
subnet mask	A code, in the form of an IP address, that computers use to determine which part of an IP address identifies the subnet and which part identifies an individual computer on that subnet.
synchronize	The process by which a handheld device and computer compare files to ensure that they contain the same data.
TCP/IP (Transmission Control Protocol/ Internet Protocol)	Standard protocols used for most Internet communication. TCP establishes connections between computers and verifies that data is properly received. IP determines how the data is routed.
threat	A program with the potential to cause damage to a computer by destruction, disclosure, modification of data, or denial of service.
Trojan horse	A program containing malicious code that is disguised as or hiding in something benign, such as a game or utility.
UDP (User Datagram Protocol)	A protocol commonly used for streaming media. Unlike TCP, UDP does not establish a connection before sending data and it does not verify that the data is properly received.
virus definition	Virus information that an antivirus program uses to identify and alert you to the presence of a specific virus.

wildcard characters

Special characters (like *, \$, and ?) that act as placeholders for one or more characters. Wildcards let you match several items with a single specification.

worm

A program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.



Index

A

access

- Block Traffic 64
- options 93
- Security Check 63
- Visual Tracking 63, 64

accounts

- creating 157, 161
- creating with Productivity Control Wizard 157
- levels 156
- logging on 163
- Not Logged In 156
- passwords 161
- set startup 161
- using Windows accounts 162

activate

- and register 47
- software 47

activation 26, 60

active content

- protection from 111
- troubleshooting 219

ActiveX controls 219

Activity Log

- checking 214
- viewing 214

Ad Blocking 186

- about 27
- enabling and disabling 71
- identifying ads to block 186

Ad Blocking 186 (*continued*)

- modifying text strings 188

Ad Trashcan 185

adding files to Quarantine 152

addresses

- adding allowed 67
- adding blocked 68
- importing allowed 67

administering Norton Internet

Security Professional

- configuring administrator computer 75
- exporting settings file 76
- importing settings file 78

Adobe Acrobat Reader

- installing 88
- using to view PDF 88

advertisements

- Ad Trashcan 185
- blocking 186
- filters 186

Alert Assistant 28, 61

alerts

- Alert Assistant 61
- Inoculation 151
- Intrusion Detection 124
- Network Detector 132
- New Location 61
- overview 61
- Worm Blocking 150

Allowed list 67

applications, accessing Internet. *See*
Internet-enabled programs

at-risk files

about 145

excluding 147

attack signatures 123, 125

attacks 64, 128

about 123

alerts 124

blocking 124

excluding 125

network 111

tracing 63, 64

from AutoBlock 64

from Statistics 64

AutoBlock 126, 128

Automatic LiveUpdate 98, 108

Automatic Program Control 116

Auto-Protect

disabling 81

enabling 135

failure to load on startup 225

functions 31

options 97

B

backing up files before repair 99

banner ads 186

Block Traffic

about 64

using 64

Blocked list 68

blocking

advertisements 71, 186

browser information 221

computers 126

cookies 179, 219

email addresses 179

spam 181

Web sites 167

by category 167

by name 168

blocking (*continued*)

Web sites 167 (*continued*)

exceptions 169

Bloodhound technology

description 32

options 97

booting

Auto-Protect failure to load 225

changing boot sequence 230

floppy disk drive fails 230

Rescue Disks fail 229

browser

information 221

privacy 179

C

cache, excluding from Web

Cleanup 204

CD-ROM drive, starting from 19

changing

feature settings 93

firewall rules 120

individual security settings 112

options 92

order of firewall rules 120

scan schedules 142

Security Level 112

checking

for recoverable files 191

for updates 93

version number 53

vulnerability to attack 62

clearing 133

computer

blocking 126

emergency procedures 17

names 121

requirements 35

specifying 121

individually 121

ranges 122

with a network address 122

- connecting to the Internet
 - automatically 108
- Connection Keep Alive
 - description 205
 - enabling and disabling 205
 - features 34
 - ISP support 205
 - settings 206
 - system tray icon 206
 - viewing status 206
- Cookie Blocking
 - options 179
 - troubleshooting 219
- cookies 179, 219
 - deleting 199, 200
 - excluding from Web Cleanup 204
- creating
 - accounts 157
 - custom virus scans 139
 - Emergency Disks 20
 - firewall rules 115
 - Rescue Disks 80
- credit card numbers 176
- custom installation 45
- custom scans
 - creating 139
 - deleting 140
 - deleting schedule 143
 - running 140
 - scheduling 141, 142
 - using 139
- customizing
 - Allowed list 67
 - Blocked list 68
 - installation 45
 - Intrusion Detection 123
 - Personal Firewall 111
 - spam filter 181

D

- data, eliminating permanently 193, 196
- default options 100
- definitions of technical terms 86
- deleting
 - cache files 200
 - cookies 199
 - custom scans 140
 - infected files 149
 - Internet temporary files 200
 - locations 134
 - scan schedules 143
- description of product features 25
- detailed statistics
 - about 211
 - categories 211
 - viewing 211
- dial-up connections, maintaining
 - with Connection Keep Alive 205
- disabling
 - Automatic LiveUpdate 109
 - Connection Keep Alive 205
 - Norton Internet Security
 - Professional 55, 79
 - Windows XP firewall 40
- disks
 - manually scanning 136
 - protecting 135
 - scanning for viruses 136
- displaying the Norton AntiVirus
 - toolbar 59
- domain names
 - excluding from Web Cleanup 203
 - using with Connection Keep Alive 207
- drive A
 - boot sequence 230
 - using for Emergency Disks 20
 - using for Rescue Disks 81, 85

E

- electronic newsletter 90
- email
 - menu 57
 - options 98
 - program, toolbar 57
 - protection 98
 - spam 181
 - supported clients 37
- emergency
 - preparations 23
 - recovery procedures 17
- Emergency Disks
 - creating 20
 - using 21
- enabling
 - Ad Blocking 71
 - Automatic LiveUpdate 106
 - Connection Keep Alive 205
 - Office Plug-in 99
 - Popup Window Blocking 72
- encryption 180
- erased files, recovering 189
- Event Log. *See* Log Viewer
- excluding at-risk files 145, 147
- Express mode for LiveUpdate 106

F

- FAQs 225
- features
 - about 27
 - Connection Keep Alive 34
 - Norton AntiVirus 31
 - Norton Internet Security
 - Professional 27
 - Web Cleanup 34
- file extensions
 - of infected files 154
 - unusual 226
- files
 - adding to Quarantine 152

files (*continued*)

- and Norton Protection 189
- check if recoverable 191
- recovering 189
- reinfected after virus
 - removal 226
- security considerations 193
- viewing with Web Cleanup 200

filtering

- and SSL 181
- changing rule priority 183
- email 66
- identifying email senders 67, 68
- training 69
- with text strings 183, 186, 187

firewall

- and LiveUpdate 107
- and network 107
- troubleshooting 219
- Windows XP 40

firewall rules

- processing order 115
- for Web servers 219

floppy drives, unable to boot

- from 230

folders

- scanning 138
- scanning for viruses 136

FTP, restricting 172

full system scans 137

G

- glossary 86

H

- Help
 - online 86
 - window and dialog box 87
- hexadecimal values, in Wipe
 - Info 194

I

- ignoring files 149
- infected files
 - cannot repair 227
 - reinfected 226
- Information Wizard
 - features 47
 - how to use 47
- Inoculation
 - alerts 151
 - options 99
 - responding to alerts 152
- installing 41
 - components 45
 - if problems are found 18
 - your product, with a virus 18
- instant messenger
 - and Privacy Control 176
 - options 98
 - protecting private information 176
 - scanning transferred files 135
 - supported programs 37
 - virus protection 32
- Interactive mode for LiveUpdate 106
- Internet
 - access statistics
 - contents 211
 - resetting 210
 - excluding history from Web Cleanup 204
 - files, cleaning 199
 - history files, deleting 200
 - Knowledge Base articles 217
 - options 97
 - Symantec service and support
 - Web site 217
 - Symantec Web sites 88
- Internet-enabled programs 117
- Intrusion Detection
 - about 27
 - configuring 124

Intrusion Detection (*continued*)

- service 104
- updates 104
- italicized terms 86

J

- Java applets 219

L

- LiveUpdate
 - Interactive and Express
 - modes 106
 - options 93, 98
 - procedure 105
- Local Networking 114, 115
 - zones 114, 115
- locations 133
 - about 130
 - adding networks 132
 - creating 130, 131
 - customizing 133
 - deleting 134
 - descriptions 130
 - Network Detector alert 132
 - removing networks from 133
- Log Viewer
 - contents 214
 - monitoring activities in 214
 - reviewing 212
 - using 212
- logs. *See* Log Viewer

M

- Managed Settings. *See* User Access Manager
- Miscellaneous options 98, 99
- mobile computing, and Network Detector 129

N

- Network Detector 129, 134
 - about 27, 129
 - adding networks to locations 132
 - creating new locations 130
 - customizing 133
 - locations 130
 - adding networks 132
 - clearing 133
 - creating 130, 131
 - customizing 133
 - deleting 134
 - Network Detector alert 132
 - removing networks from 133
- networks
 - configuring with Workgroup Networking Wizard 114
 - internal LiveUpdate server 107
 - troubleshooting 220
 - using LiveUpdate 107
- new features in Norton AntiVirus 31
- newsgroups, exceptions 173
- newsletters 90
- Norton AntiSpam 181
 - about 28
 - Allowed and Blocked lists 29
 - and SSL 181
 - customizing 181
 - enabling and disabling 66
 - features 29
 - modify entry 182
 - troubleshooting 222
- Norton AntiVirus
 - Auto-Protect 31
 - Bloodhound technology 32
 - customizing 96
 - starting from the main window 58
 - starting from the Windows Explorer toolbar 58
 - starting from the Windows system tray 58
 - Norton AntiVirus (*continued*)
 - virus protection 31
 - virus protection updates 31
- Norton Internet Security
 - Firewall options 94
 - General options 93
- Norton Internet Security Professional
 - creating accounts 157, 161
 - disabling 79
 - Log Viewer 209
 - logging on 163
 - monitoring 209
 - statistics 209
 - Visual Tracking 63, 64
- Norton Personal Firewall, LiveUpdate options 93
- Norton Protection 33, 189
- Norton SystemWorks features
 - Connection Keep Alive 34
 - Web Cleanup 34
- Norton Tray Manager, Connection Keep Alive icon 205
- Norton Tray Manager, and Connection Keep Alive icon 206
- Norton Utilities
 - Norton Protection 33
 - Recycle Bin protection 33
 - UnErase Wizard 33
 - Wipe Info 33

O

- Office Plug-in
 - enabling 99
 - status 73
- online
 - Help 86
 - Virus Encyclopedia 154
- operating systems 35
 - multiple 229
- Options
 - Connection Keep Alive 206
 - Wipe Info 102

- options 91
 - accessing 93
 - Auto-Protect
 - Advanced 97
 - Bloodhound 97
 - Exclusions 97
 - categories 96
 - changing 100
 - changing settings for 96
 - customizing 96
 - email
 - Advanced 98
 - scanning 98
 - Inoculation 99
 - instant messenger 98
 - Internet 97
 - LiveUpdate 93, 98
 - Manual Scan
 - Bloodhound 97
 - Exclusions 97
 - Miscellaneous 98, 99
 - Norton Internet Security
 - Firewall 94
 - General 93
 - Norton Personal Firewall,
 - LiveUpdate 93
 - Other 98
 - password protection in Norton
 - AntiVirus 32
 - protecting with password 94
 - resetting defaults 100
 - resetting password 95
 - Threat Categories 99
 - Wipe Info 195
 - Worm Blocking 98
- Other options 98

P

- password protection option 99
- passwords
 - changing 161
 - resetting 95
- passwords (*continued*)
 - setting 161
- Personal Firewall
 - about 27, 111
 - customizing 115
 - security settings 112
 - troubleshooting rules 219
- pinging with Connection Keep Alive 207
- Popup Window Blocking
 - about 30
 - and Web assistant 62
 - enabling and disabling 72
 - troubleshooting 224
- port scans 111
- Privacy Control
 - about 27, 175
 - and secure Web connections 180
 - Browser Privacy 179
 - Cookie Blocking 179
 - in instant messengers 176
 - private information
 - adding 176
 - modifying 176
 - Private Information setting 178
 - using with HTTPS 180
- private information
 - adding 176
 - modifying 176
 - options 178
- problems
 - troubleshooting Norton
 - AntiSpam 222
 - troubleshooting Norton
 - AntiVirus 225
 - troubleshooting Norton Internet Security Professional 219
 - troubleshooting Rescue
 - Disks 229
- product key 26
- Productivity Control
 - about 28

Productivity Control (*continued*)

creating accounts 157, 161

Wizard 157

program

patches 103

updates 103

Program Control 116

Automatic 116

manually adding programs 118

scanning for programs 117

settings 118

Program Scan

configuring 117

running 117

programs

See also Internet-enabled

programs

configuring with Program

Scan 117

creating firewall rules 119

manually adding to Program

Control 118

manually configuring Internet

access 119

protection

downloading from Symantec Web

site 105

maintaining 22

maximum 135

preparing for emergencies 23

system scans 137

updating 108

protection updates defined 104

proxy servers 219

Q

Quarantine

actions in 152

adding files to 152

files in 152

infected files in 148

options 152

Quarantine (*continued*)

restoring items 152

R

Readme file 87

Recycle Bin

and Norton Protection 189

protected by Norton Protection 33

recovering files from 191

register your software 47

removing

Ad Blocking strings 187

Norton AntiVirus 50

Norton Internet Security

Professional 50

other antivirus programs 40

previous copies of Norton Internet

Security 40

spam rules 182

Repair Wizard 146

repairing

infected files

in Windows 2000/XP 149

in Windows 98/98SE/Me 148

viruses 31

required computer configuration 35

Rescue Disks

creating 80

creating folder on hard disk 81

disabling Auto-Protect 81

failure to start from 229

not current 85

supported platforms 80

testing 82

troubleshooting 229

updating 83

using 84

restarting

after installation 45

and Block Traffic 65

Windows in safe mode 225

- restoring
 - items in Quarantine 152
 - system with Inoculation 99
 - system with Rescue Disks 84

- risks
 - intrusions 111
 - port scans 111

S

- safe mode 225

- scan summary 146

- scanning

- Automatic Program Control 116
 - automatically 141
 - before installation 41
 - email messages 98
 - entire computer 137
 - files at startup 99
 - for Internet-enabled programs 116
 - individual elements 138
 - port 111
 - problems found during 138

- scans

- creating custom 139
 - deleting custom 140
 - file 138
 - floppy disk 138
 - folder 138
 - full system 137
 - hard drive 138
 - removable drive 138
 - running custom 140
 - using custom 139

- scheduling

- custom scans 141
 - multiple schedules for a scan 142
 - virus scans 141

- secure Web connections, disabling and enabling 180

- security

- attacks 123, 128

- security (*continued*)

- levels 112

- Security Check 62

- Security Level

- changing 112

- changing individual settings 112

- Security Response Web page 89

- security risks

- attacks 111, 123

- finding 145

- port scans 111

- Service and Support 233

- settings

- Connection Keep Alive 206

- exporting 75

- Personal Firewall 112

- Program Control 118

- transferring to other

- computers 75-78

- using Windows accounts 76

- Setup program, changing boot drive sequence 230

- spam

- blocking 181

- filters 183

- changing priority 183

- modifying 182

- SSL (Secure Sockets Layer), and

- Norton AntiSpam 181

- starting

- Ad Blocking 71

- can't start your computer 18

- from the CD-ROM drive 19

- Norton AntiVirus 58

- virus preventing computer from 84

- startup

- alert about virus protection 99

- Auto-Protect failure to load 225

- changing boot sequence 230

- floppy disk drive fails 230

- Rescue Disks fail 229

- startup (*continued*)
 - scanning files at 99
- statistics 211
 - detailed 211
 - Norton Internet Security Professional 209
 - resetting 210
 - viewing 210
- statistics window 210
- stopping
 - Ad Blocking 71
 - communications with Block Traffic 64
- submitting
 - files to Symantec 153
 - Web sites to Symantec 171
- subnet masks 122
- subscription to product updates 110
- summary of product features 25
- Symantec Pre-Install Scanner 18, 41
- Symantec Security Response
 - newsletter 90
 - Web page 59
 - Web site 89
- Symantec service and support Web site 217
- Symantec Web sites 88, 105
 - connecting to 59
 - look up viruses 154
- system requirements 35
- system status, checking 73
- system tray icons
 - Connection Keep Alive 206
 - Norton Internet Security Professional 55

T

Technical Support 88, 233

threats

- attacks 123
- avoiding 22
- categories of 99

threats (*continued*)

- expanded detection of 31
- found by manual scan 145
- protection from 111
- timeout protection 136
- toolbar, displaying Norton AntiVirus from 59
- training Norton AntiSpam 69
- Trashcan. *See* Ad Trashcan
- tray icon 55
- Trojan horses, found during a scan 146
- troubleshooting 217
 - ActiveX and Java 219
 - Ad Blocking 224
 - browser information 221
 - Cookie Blocking 219
 - firewall rules 219
 - networks 220
 - Norton AntiSpam 222
 - Norton AntiVirus 225
 - printing 220
 - recovering erased files 189
 - Rescue Disks 229
 - Web sites 219

U

UnErase Wizard 33

- features 190
- recovering files with 191

Uniform Resource Locator (URL) 121

uninstalling 50

- Norton AntiVirus 50

- Norton Internet Security Professional 50

- other antivirus programs 40

- previous copies of Norton Internet Security 40

unknown viruses 32

updating

- from Symantec Web site 105
- Rescue Disks 83

- updating (*continued*)
 - virus protection 105
- URLs (Uniform Resource Locators)
 - about 121
 - limiting access 171
- URLs, saving from Web Cleanup 203
- User Access Manager
 - about 28
 - exporting settings 76
 - importing settings 78
- User's Guide PDFs
 - on CD 88
 - opening 88

V

- version number, checking 53
- virtual private network (VPN) 38
- virus alert options 148
- Virus Encyclopedia 59, 89
- virus protection
 - alerts 99
 - system scans 137
 - updates 31
- virus repair
 - in Windows 2000/XP 149
 - in Windows 98/98SE/Me 148
- viruses
 - automatic protection 31
 - avoiding 22
 - descriptions 31
 - found by Auto-Protect 148
 - found during a scan 146
 - looking up on the Symantec Web site 154
 - submitting to Symantec 153
 - unknown 32
 - viewing descriptions 154
- Visual Tracking 63, 64
 - trace attack
 - from AutoBlock 64
 - from Statistics 64
- VPN (virtual private network) 38

W

- Web
 - filtering service 104
 - sites
 - blocking 167
 - submitting to Symantec 171
 - troubleshooting 219
 - sites, Symantec 88, 105, 217
- Web assistant
 - about 27, 62
 - using 62
 - viewing 62
- Web Cleanup 199
 - excluding files from cleanup 204
 - features 34
 - file viewer 200
 - options 204
 - saving URLs 203
- Web Tools
 - Connection Keep Alive 34
 - using 199-208
 - Web Cleanup 34
- Windows
 - operating systems 35
 - safe mode 225
- Windows 2000
 - system requirements 36
 - Wipe Info procedure 196
- Windows 98/98SE/Me, system requirements 36
- Windows Explorer toolbar, displaying
 - Norton AntiVirus 58
- Windows Me, system requirements 36
- Windows system tray, Connection Keep Alive icon 205
- Windows XP
 - system requirements 36
 - System Restore after Wipe Info 193
 - Wipe Info procedure 196

Wipe Info

- and Windows Me/XP System

- Restore 193

- characters used to wipe 194

- features 33

- Government Wipe 194

- on Windows 2000/XP 196

- options 102, 195

- procedures 193, 196

wizards

- Productivity Control 157

- Repair 146

- UnErase 190

Workgroup Networking

- about 114

- configuration 114

Worm Blocking

- monitoring by 135

- Norton AntiVirus 32

- options 98

- threats found by 150

worms

- found by Worm Blocking 150

- found during a scan 146

- in email messages 98, 150

- in Microsoft Office documents 73

Z

- zones 114, 115

- Restricted 114, 128

- Trusted 114, 123